A Joint Standard of AASHTO, ITE, and NEMA

NTCIP 1218 v01.38

National Transportation Communications for ITS Protocol

Object Definitions for Roadside Units (RSUs)

Published in September, 2020

Published by

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

Institute of Transportation Engineers (ITE)
1627 Eye Street, N.W., Suite 600
Washington, D.C. 20006

National Electrical Manufacturers Association (NEMA)
1300 North 17th Street, Suite 900
Rosslyn, Virginia 22209-3801

<This page intentionally left blank.>

NOTICES

Copyright Notice

© 2020 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;
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:

a) each copy you make or distribute includes the citation “Derived from NTCIP 0000 [insert the standard number]. Copyright by AASHTO / ITE / NEMA. Used by permission.”;

b) the copies or derivative works are not made part of the standard publications or works offered by other standard developing organizations or publishers or as works-for-hire not associated with commercial hardware or software products intended for field implementation;
c) use of the DD or MIB is restricted in that the SYNTAX fields may only be modified to define: 1) a more restrictive subrange; or 2) a subset of the standard enumerated values; or 3) a set of retired and defined enumerated values for systems supporting multiversion interoperability;
d) the description field may be modified but only to the extent that: 1) the more restrictive subrange is defined; and 2) only those bit values or enumerated values that are supported are listed. [from 8002 A2 v04]

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 the user is unwilling to accept the foregoing restrictions, he or she 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 Protocol Requirements List ("PRL") or a Requirements Traceability Matrix ("RTM"), AASHTO / ITE / NEMA extend the following permission:

a) 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 standard number] PRL or RTM. Used by permission. Original text © AASHTO / ITE / NEMA.";
b) you may only modify the PRL or the RTM by adding: 1) 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; and/or 2) additional table columns or table rows that are clearly labeled as ADDITIONAL for project-unique or vendor-unique features; and
c) if the PRL or RTM excerpt is made from an unapproved draft, add to the citation "PRL (or RTM) excerpted from a draft standard 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 PRL 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 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 fulfill 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.

Acknowledgements

NTCIP 1218 v01 was prepared by the NTCIP Roadside Unit Working Group (RSU WG), which is a subdivision of the NTCIP Joint Committee. The NTCIP 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 NTCIP Joint Committee consists of six representatives from each of the standards organizations, and provides guidance for NTCIP development. In addition, both the Society of Automotive Engineers (SAE) and IEEE provided liaison assistance in development.

When NTCIP 1218 v01 was prepared, the following individuals were voting members (indicated by an '*') or alternate voting members of the NTCIP RSU WG:

- Applied Information, Inc., Walt Townsend,* Alan Clelland, Alan Luchuk
- City of Anaheim, John Thai* (Co-Chair)
- Econolite Control Products, Inc., Gary Duncan*, Dustin DeVoe, Greg Mizell, Jim Rose
- Florida DOT, Derek Vollmer*, Jeffrey Morgan, Matthew DeWitt, Raj Ponnaluri
- Maricopa County AZ DOT, Faisal Saleem*
- Michigan DOT, Joe Gorman*, Colin Castle
- Parsons, Jon Wyatt* (Co-Chair)
- Siemens Industry, Inc., Wolfgang Buckel*, Michael Venus
- Washington State DOT, Michael Forbis*, Mark Morse

Observing members include:

- Cal Poly-Pomona, Xinkai Wu
- Intelight Inc., Doug Crawford, Craig Gardner, Douglas Tarico
- Kapsch, Rob Bailey, Joerg Rosenbohm
- Miovision Technologies, Jan Bergstrom, J. Shantz, Kourtney Short
- SwRI Southwest Research Institute, Michael Brown, Richard Downs, Cameron Mott
- Trafficware, Theresa Rohlfs

Additional stakeholders include:

- Connected Signals, Peter Flier, Matthew Ginsberg
- CA DOT (CalTrans) PATH/UC Berkeley, Kun Zhou
- Commsignia, Inc., Alex Badics, András Takács, László Virág
- Consensus Systems Technologies, Scott Altman, Patrick Chan, Manny Insignares
- Danlaw, Mostafa Kassem
- Econolite, Dustin DeVoe
- eTrans Systems, Rob Bailey
- FLIR, David St. Claire
- Gridaptive, Jim Frazer
- HNTB, Stephen Novosad
- JMCRota, Justin McNew
- KLD Engineering, P.C., Wuping Xin
- Lear Corporation, Nazeer Shaik
- Leidos Engineering, LLC, Zhitong Huang, Edward, Leslie
- Live Traffic Data, Bryan Ferguson
- Mississippi State University, Li Zhang
- Mixon Hill, Lee Mixon
- MN DOT, Terry Haukom, Ray Starr
- Neara Consulting, Tony English
- NOKIA, Doug Hohulin
- NYC DOT, Rami Khashashina
- OmniAir Consortium, Randy Roebuck, Arthur Moore
- OR DOT, Doug Spencer
- Panasonic North America, Brett Kahn, Michael Stelts, Rob Zimmer
- Pillar Consulting, Ralph Boaz
- Qualcomm, Jim Misener
- Savari, Navin Katta
- SCSC, David Kelley
- Stantec, Kyle Irvin
- SwRI Southwest Research Institute, Richard Downs, Cameron Mott
- The University of Arizona, Larry Head

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

- Trafficast, Paul Misticawi, Kent Ragay
- Transcore, ITS, David Benevelli, Robert Rausch
- Transurban, Patrick Chuang
- Trevilon Corp., Kenneth Vaughn
- Triunity Engineering & Management, Israel Lopez
- Western Systems Inc., Donald Wang
- WSP, Anthony Gasiorowski, Frank Perry, Brian Reed, Thomas Timcho

In addition to the many volunteer efforts, recognition is also given to those organizations that supported the effort by providing funding:

- U.S. Department of Transportation

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

Foreword

NTCIP 1218 v01, an NTCIP standards publication, identifies and defines how a management station interfaces with a roadside unit (RSU), in an NTCIP-conformant fashion. NTCIP 1218 v01 uses only metric units. A roadside unit is a field device that serves as a demarcation point between connected devices, such as vehicles or mobile devices (e.g., smartphones), and the road infrastructure in a Cooperative Intelligent Transport Systems (C-ITS) environment. NTCIP 1218 v01 strives to be communications agnostic, that is, NTCIP 1218 v01 does not dictate what communications media is used between the connected devices and the road infrastructure. NTCIP 1218 v01 does not intend to preclude any communications media (specific technologies or formats), but focuses on the well-known and well-understood communications media that were considered suitable for its intended purpose at the time of development/publication.

NTCIP 1218 v01 is titled *Object Definitions for Roadside Units (RSUs)*.

NTCIP 1218 v01 defines data objects for use with RSUs. The data is defined using the Simple Network Management Protocol (SNMP) OBJECT-TYPE macro format as defined in RFC 2578.

NTCIP 1218 v01 follows an established systems engineering approach to support procurement processes. The Protocol Requirements List (PRL) allows an agency to indicate which user needs are applicable in a unique agency specification, and to select which requirements are to be implemented in a project-specific context. Proper completion of the PRL by the agency results in an agency specification that is more likely to satisfy the agency's project needs and that is conformant to NTCIP 1218 v01. The Requirements Traceability Matrix (RTM) identifies the dialogs and objects that fulfill those requirements selected, and may also be used to develop test plans and test procedures.

The following keywords apply to this document: AASHTO, ITE, NEMA, NTCIP, data, data dictionary, object, MIB, PRL, RSU, and RTM.

NTCIP 1218 v01 is also an NTCIP Data Dictionary standard. Data Dictionary standards provide definitions of data concepts (messages, data frames, and data elements) for use within NTCIP systems; and are approved by AASHTO, ITE, and NEMA through a ballot process, after a recommendation by the NTCIP Joint Committee. For more information about NTCIP standards, or to acquire the related NTCIP 1218 v01 MIB, visit 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 NTCIP 1218 v01 content. A "Request for Interpretation" 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.

User Comments are generally referred to the committee responsible for developing and/or maintaining NTCIP 1218 v01. 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 is 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.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

A User Comment should be submitted to this address:

NTCIP Coordinator
National Electrical Manufacturers Association
1300 North 17th Street, Suite 900
Rosslyn, Virginia 22209-3801
e-mail: ntcip@nema.org

A User Comment should be submitted in the following form:

Standard Publication number and version:
Section, Paragraph:
Editorial or Substantive?:
Suggested Alternative Language:
Reason:

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

Approvals

NTCIP 1218 v01 was separately balloted and approved by AASHTO, ITE, and NEMA after recommendation by the Joint Committee on the NTCIP. Each organization has approved NTCIP 1218 v01 as the following standard type, as of the date:

AASHTO—Standard Specification; April, 2020
ITE—Software Standard; April, 2020
NEMA—Standard; July, 2020

History

In 1992, the NEMA 3TS Transportation Management Systems and Associated Control Devices Section began the effort to develop NTCIP. 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 ITS network.

In September 1996, an agreement was executed among AASHTO, ITE, and NEMA to jointly develop, approve, and maintain the NTCIP standards. In late 2017, the Roadside Unit (RSU) Working Group was tasked with the effort to develop NTCIP 1218 v01.

Compatibility of Versions

To distinguish NTCIP 1218 v01 (as published) from previous drafts, NTCIP 1218 v01 also includes NTCIP 1218 v01.38 on each page header. All NTCIP Standards Publications have a major and minor version number for configuration management. The version number SYNTAX is "v00.00a," with the major version number before the period, and the minor version number and edition letter (if any) after the period.

NTCIP 1218 v01 is designated, and should be cited as, NTCIP 1218 v01. Anyone using NTCIP 1218 v01 should seek information about the version number that is of interest to them in any given circumstance. The PRL, RTM and the MIB should all reference the version number of the standards publication that was the source of the excerpted material.

Compliant systems based on later, or higher, version numbers MAY NOT be compatible with compliant systems based on earlier, or lower, version numbers.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

CONTENTS

Page

Section 1 General [Informative] 1
1.1 Scope 1
1.2 References 2
1.2.1 Normative References 2
1.2.2 Other References 4
1.2.3 Contact Information 5
1.3 General Statements 6
1.4 Terms 6
1.5 Abbreviations 8
Section 2 Concept of Operations [Normative] 10
2.1 Tutorial [Informative] 10
2.2 Current Situation and Problem Statement [Informative] 12
2.3 Reference Physical Architecture [Informative] 12
2.3.1 RSU Characteristics - General 14
2.3.2 RSU Characteristics - V2X Radio Type 16
2.4 Architectural Needs 16
2.4.1 Configure, Monitor and Control the RSU 17
2.4.2 Provide for Log Data Local Storage and Retrieval 17
2.4.3 Condition-based Exception Reporting 17
2.5 Features 17
2.5.1 Manage the RSU Configuration 17
2.5.2 Monitor the RSU 21
2.5.3 Control the RSU 22
2.6 Security 23
2.6.1 Manage Authentication 23
2.6.2 Manage Data Integrity 23
2.6.3 Manage Availability 23
2.6.4 Manage Confidentiality 23
2.7 Operational Policies and Constraints 23
2.8 Relationship to the ITS National Architecture [Informative] 24
Section 3 Functional Requirements [Normative] 27
3.1 Tutorial [Informative] 27
3.2 Scope of The Interface [Informative] 28
3.3 Protocol Requirements List (PRL) 28
3.3.1 Notation [Informative] 29
3.3.2 Instructions for Completing the PRL [Informative] 30
3.3.3 Protocol Requirements List (PRL) Table 31
3.4 Architectural Requirements 47
3.4.1 Support Basic Communications Requirements 47
3.4.2 Log Data Local Storage and Retrieval Requirements 47
3.4.3 Condition-based Exception Reporting 48
3.5 Data Exchange and Operational Environment Requirements 48
3.5.1 RSU Configuration Management Requirements 48
3.5.2 RSU Monitoring Requirements 68
3.5.3 RSU Control Requirements 75

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

3.5.4 Security Requirements 75
3.6 Supplemental Non-communications Requirements 76
3.6.1 Security Requirements 76
3.6.2 Response Time for Requests 77
3.6.3 Event Log Data Requirements 77
3.6.4 Interface Data Log Data Requirements 79
3.6.5 Copy Files using SCP 80
3.6.6 User Accounts 80
3.6.7 Time Fix - Alternating Mode 80
3.6.8 Determine Maximum Number of Application Certificates Supported 80
Section 4 Dialogs [Normative] 81
4.1 Tutorial [Informative] 82
4.2 Specified Dialogs 83
4.2.1 Generic Retrieve Table Dialog - Static Table 83
4.2.2 Generic Retrieve Table Row Dialog 83
4.2.3 Generic Configure Table Row Dialog 84
4.2.4 Generic Retrieve Table Dialog - Dynamic Table 84
4.2.5 Secure Copy Protocol Dialog 84
4.2.6 Secure Installation Dialog 85
4.2.7 Retrieve Event Logged Data Dialog 85
4.3 State-Transition Diagrams 86
4.3.1 Operating Mode State Machine Definition 86
Section 5 Management Information Base (MIB) [Normative] 87
5.1 MIB Header 87
5.2 RSU Radios 88
5.2.1 Maximum Radios 88
5.2.2 Radio Table 89
5.3 RSU GNSS 92
5.3.1 GNSS Status 92
5.3.2 GNSS Augmentation 93
5.4 Store and Repeat Messages 93
5.4.1 Maximum Number of Store and Repeat Messages 93
5.4.2 Store and Repeat Table 93
5.4.3 Delete All Stored Messages 96
5.5 Immediate Forward Messages 97
5.5.1 Maximum Number of Immediate Forward Messages 97
5.5.2 Immediate Forward Table 97
5.6 Received Messages 100
5.6.1 Maximum Number of Messages 100
5.6.2 Received Messages Table 100
5.7 GNSS Output 104
5.7.1 GNSS Output Port 104
5.7.2 GNSS Output Address 104
5.7.3 GNSS Output Interface Description 104
5.7.4 GNSS Output Interval 105
5.7.5 GNSS Data Output 105
5.7.6 GNSS Reported Latitude 105
5.7.7 GNSS Reported Longitude 105
5.7.8 GNSS Reported Elevation 106
5.7.9 GNSS Allowable Location Deviation 106
5.7.10 GNSS Location Deviation 106
5.7.11 RSU Position Error 106

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

5.8 Interface Log 107
5.8.1 Maximum Number of Interface Logs 107
5.8.2 Interface Log Table 107
5.9 Security 111
5.9.1 Security Credentials Request 111
5.9.2 Enrollment Certificate Status 111
5.9.3 Enrollment Certificate Valid Region 111
5.9.4 Enrollment Certificate Source Domain 111
5.9.5 Enrollment Certificate Identifier 112
5.9.6 Enrollment Certificate Expiration 112
5.9.7 Enrollment Certificate Source 112
5.9.8 Application Certificate Source 112
5.9.9 Maximum Application Certificates 112
5.9.10 Application Certificate Table 113
5.9.11 Certificate Revocation List Source 115
5.9.12 Certificate Revocation List Update Time 115
5.9.13 Certificate Revocation Update Interval 115
5.9.14 Certificate Revocation List Command 115
5.9.15 Maximum Number of Security Profile Entries 115
5.9.16 Security Profiles 116
5.10 WAVE Service Advertisement 117
5.10.1 Maximum Number of WSA Services 117
5.10.2 WAVE Service Advertisement Service Table 117
5.10.3 WAVE Service Advertisement Channel Table 122
5.10.4 WAVE Service Advertisement Version 124
5.11 WAVE Router Advertisement Configuration 124
5.11.1 WAVE Router Advertisement Prefix 124
5.11.2 WAVE Router Advertisement Prefix Length 125
5.11.3 WAVE Router Advertisement Gateway 125
5.11.4 WAVE Router Advertisement Primary DNS 125
5.11.5 WAVE Router Advertisement Secondary DNS 125
5.11.6 WAVE Router Advertisement Gateway MAC 126
5.11.7 WAVE Router Advertisement Lifetime 126
5.12 Message Statistics 126
5.12.1 Maximum Number of Message Counts by PSID 126
5.12.2 RSU Message Count Table 126
5.13 Systems Statistics 128
5.13.1 Time Since RSU Powered On 129
5.13.2 RSU Internal Temperature 129
5.13.3 RSU Internal Temperature - Low Temperature Warning 129
5.13.4 RSU Internal Temperature - High Temperature Warning 129
5.13.5 Maximum Number of Communications Range Entries 130
5.13.6 RSU Communications Range Table 130
5.14 System Description 134
5.14.1 RSU MIB Version 134
5.14.2 RSU Firmware Version 134
5.14.3 RSU Location Description 134
5.14.4 RSU Identifier 134
5.14.5 RSU Reference Location - Latitude 135
5.14.6 RSU Reference Location - Longitude 135
5.14.7 RSU Reference Location - Elevation 135
5.14.8 RSU Reference Location - Elevation Offset 135
5.14.9 RSU Installation Command 136
5.14.10 RSU Installation Filename 136

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

5.14.11 RSU Installation Path 136
5.14.12 RSU Installation Status 137
5.14.13 RSU Installation Status Time 137
5.14.14 RSU Installation Status Message 137
5.14.15 RSU Scheduled Installation Time 137
5.15 System Settings 138
5.15.1 Notification Destination Address 138
5.15.2 Notification Destination Port 138
5.15.3 System Log Query Start Time 138
5.15.4 System Log Query Stop Time 138
5.15.5 System Log Query Priority 139
5.15.6 System Log Query Generate 139
5.15.7 System Log Query Status 139
5.15.8 System Log Close Command 140
5.15.9 System Log Severity 140
5.15.10 System Configuration File 140
5.15.11 System Startup Retries 140
5.15.12 System Startup Retry Period 141
5.15.13 Short Communications Loss Time 141
5.15.14 Long Communications Loss Time 141
5.15.15 System Log Name 142
5.15.16 System Base Directory 142
5.15.17 Long Communications Loss Reboot 142
5.15.18 RSU Host Network Address Parameter 143
5.15.19 RSU Host Net Mask Parameter 143
5.15.20 RSU Host Gateway Parameter 143
5.15.21 RSU Host Domain Name Server Parameter 144
5.15.22 RSU Host DHCP Enable Parameter 144
5.16 Antenna Settings 144
5.16.1 Maximum Antennas 144
5.16.2 Antenna Table 145
5.17 RSU System Status 147
5.17.1 RSU Radio Status 147
5.17.2 RSU Mode 147
5.17.3 RSU Mode Status 147
5.17.4 RSU Reboot 148
5.17.5 RSU Clock Source 148
5.17.6 RSU Clock Status 148
5.17.7 RSU Clock Source Timeout 148
5.17.8 RSU Clock Source Queries 149
5.17.9 RSU Clock Deviation Tolerance 149
5.17.10 RSU System Status 149
5.18 Asynchronous Message 150
5.18.1 Notifications 150
5.18.2 Notification Objects 152
5.18.3 Notification Repeat Interval 156
5.18.4 Notification Maximum Retransmission Retries 156
5.19 RSU Applications 156
5.19.1 Maximum Applications 156
5.19.2 RSU Application Configuration Table 156
5.20 RSU Services 158
5.20.1 Maximum RSU Service Entries 158
5.20.2 RSU Services Table 159
5.21 Transmitted Messages For Forwarding 161

 © 2020 AASHTO / ITE / NEMA

5.21.1 Maximum Number of Transmitted Messages for Forwarding 161
5.21.2 Transmitted Messages for Forwarding Table 161

Annex A Requirements Traceability Matrix (RTM) [Normative] 165

A.1 Notation [Informative] 165
A.1.1 Functional Requirement Columns 165
A.1.2 Dialog Column 165
A.1.3 Object Columns 166
A.1.4 Additional Specifications 166
A.2 Instructions For Completing The RTM [Informative] 166
A.3 Requirements Traceability Matrix (RTM) Table 166

Annex B Object Tree [Informative] 207

Annex C Test Procedures [Normative] 209

Annex D Documentation of Revisions [Informative] 210

Annex E User Requests [Informative] 211

E.1 Approach 211
E.2 Perform Diagnostics 211
E.3 Manage RSU Initialization Functions 211
E.3.1 User Need - Manage RSU Initialization Functions 211
E.3.2 Requirement - Mandatory Applications 211
E.4 RSU Master - Slave 212
E.4.1 Requirement - Store RSU Master - Slave Assignment 212
E.4.2 Requirement - Store RSU Master - Slave Role 212
E.4.3 Requirement - Store RSU Slave Address 212
E.4.4 Requirement - Store RSU Master Address 212
E.5 Report Firmware Update Status Options 212
E.6 Encrypting Messages Transmitted Over the V2X Interface 212
E.7 Signing Messages Transmitted Over the V2X Interface 213
E.8 Encoding Messages Transmitted Over the V2X Interface 213
E.9 Manage Scheduler 213
E.10 Security 213
E.11 RSU Component Information 213
E.12 RSU Edge Computing 214
E.13 RSU Firmware Update of Mobile Devices 214
E.14 Valid Geographic Region for Application Certificates 214
E.15 Event Log - User-Defined Events 214
E.15.1 Requirement - Event Log - Configure User-Defined Events 214
E.15.2 Requirement - Event Log - User-Defined Events 215
E.15.3 Requirement - Event Log - Configure User-Defined Conditions - Received Message on the V2X Interface 215
E.15.4 Requirement - Event Log - User-Defined Conditions - Received Messages on the V2X Interface 215
E.15.5 Requirement - Event Log Priority Levels 215
E.15.6 Supplemental Requirement - Record and Timestamp Events 215
E.15.7 Supplemental Requirement - Support On-Change Events 215
E.15.8 Supplemental Requirement - Support Greater Than Events 215
E.15.9 Supplemental Requirement - Support Less Than Events 215
E.15.10 Supplemental Requirement - Support Hysteresis Events 215
E.15.11 Supplemental Requirement - Support Periodic Events 215
E.15.12 Supplemental Requirement - Support Bit Flag Events 216

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

E.15.13 Supplemental Requirement - Support Event Monitoring on Any Data 216
E.16 Requirement - Device Installation Date 216
E.17 Requirement - Encoding Formats 216
E.18 UDP Port for Immediate Forwarding 216
E.19 Clock Skew Rate 216
E.20 Radios Broadcasting on the Same Channel 217
E.21 Monitor Electrical Power 217
E.21.1 Requirement - Monitor Electrical Voltage 217
E.21.2 Requirement - Monitor Electrical Current 217
E.21.3 Requirement - Determine Electrical Voltage Threshold 217
E.21.4 Object Definition - RSU Electrical Voltage 217
E.21.5 Object Definition - RSU Electrical Amperage 217
E.21.6 Object Definition - RSU Electrical Voltage - Low Voltage Warning 218
E.22 Notification - Certificate Management Warnings 218
E.23 IEEE 802.1X 218
E.24 Factory Default 218
E.25 Forwarding Messages Received from or Transmitted to the V2X Interface using TCP 218
E.26 Standalone Mode 218
Annex F Generic Concepts and Definitions 220
Annex G SNMP Interface [Normative] 221
G.1 Generic SNMP Get Interface 221
G.2 Generic SNMP Get-Next Interface 221
G.3 Generic SNMP Set Interface 222
G.4 Variable Binding List Structure 223
G.5 Additional Requirements 223
G.5.1 Grouping of Objects in a Request 223
G.5.2 Support of Get 223
G.5.3 Support of Get-Next 223
G.5.4 Support of Set 223
G.5.5 Performance 224
G.5.6 Properly Defined Objects 224
G.6 Generic SNMP Trap Interface 224

 © 2020 AASHTO / ITE / NEMA

FIGURES

Page
Figure 1 Reference Physical Architecture: RSU System 13
Figure 2 RSU Context Diagram 14
Figure 3 RSU Alternate Context Diagram 16
Figure 4 SET-IT Diagram for NTCIP 1218 v01 24
Figure 5 ARC-IT Physical View 26
Figure 6 IEEE 802.11 Channel Number Mapping 57
Figure 7 Object Tree for NTCIP 1218 v01 207
Figure 8 SNMP Get Interface 221
Figure 9 SNMP GetNext Interface 222
Figure 10 SNMP Set Interface 222
Figure 11 SNMP Interface - View of Participating Classes 223
Figure 12 SNMP Trap Interface 224

TABLES

Page
Table 1 Data Flows from ARC-IT 25
Table 2 Conformance Symbols 29
Table 3 Conditional Status Notation 29
Table 4 Predicate Mapping to NTCIP 1218 v01 Section 30
Table 5 Support Column Entries 30
Table 6 Protocol Requirements List (PRL) 33
Table 7 3GPP Channel Number Mapping to IEEE 802.11 Channel Number 57
Table 8 Requirements Traceability Matrix (RTM) 166

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

<This page intentionally left blank.>

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

Section 1
General [Informative]

1.1 Scope

NTCIP 1218 v01 specifies the logical interface between an RSU and the controlling management stations. NTCIP 1218 v01 defines information that may be exchanged across this interface. NTCIP 1218 v01 first identifies the relevant RSU users and their needs, defines requirements that enable information exchanges that supports those needs, and finally defines the data objects and meta-data, including the relative structure of that data, necessary to meet these requirements.

Cooperative Intelligent Transport Systems (C-ITS) is a surface transportation environment where connected devices, such as vehicles or mobile devices (e.g., smartphones) interact or "talk" directly with each other, and the road infrastructure (which may or may not be owned by an agency). Known as connected vehicles in the United States, this environment could dramatically reduce the number of fatalities and injuries on the roadways, while improving mobility and environmental impacts.

The roadside unit (RSU) is a key enabling component of the C-ITS environment - it serves as an interface, also known as vehicle-to-infrastructure (V2I) interface, between connected devices and the roadway infrastructure. The U.S. Federal Communications Commission (FCC), at 47 CFR Part 90 (90.7), defines an RSU as:

> "…a DSRC transceiver that is mounted along a road or pedestrian passageway. An RSU may also be mounted on a vehicle or is hand carried, but it may only operate when the vehicle or handcarried unit is stationary. Furthermore, an RSU operating under this part is restricted to the location where it is licensed to operate. However, portable or hand-held RSUs are permitted to operate where they do not interfere with a site licensed operation. An RSU broadcasts data to OBUs [On-Board Units] or exchanges data with OBUs in its communications zone. An RSU also provides channel assignments and operating instructions to OBUs in its communications zone, when required."

And an On-Board Unit (OBU) as,

> "…a DSRC transceiver that is that is normally mounted in or on a vehicle, or which in some instances may be a portable unit. An OBU can be operational while a vehicle or person is either mobile or stationary. The OBUs receive and contend for time to transmit on one or more radio frequency (RF) channels. Except where specifically excluded, OBU operation is permitted wherever vehicle operation or human passage is permitted. The OBUs mounted in vehicles are licensed by rule under part 95 of this chapter and communicate with Roadside Units (RSUs) and other OBUs. Portable OBUs are also licensed by rule under part 95 of this chapter. OBU operations in the Unlicensed National Information Infrastructure (UNII) Bands follow the rules in those bands."

Although the FCC defined an RSU and an OBU as DSRC transceivers, NTCIP 1218 v01 is agnostic on the form of the communications media among the connected devices and road infrastructure. NTCIP 1218 v01 focuses on the well-known and well-understood communications media that were suitable for its intended purpose at the time, but is written to not preclude any future communications media. As such, the transceivers to interface with connected devices are called V2X transceivers throughout NTCIP 1218 v01.

Prior to the development of NTCIP 1218 v01, there was no NTCIP standard fully defining how RSUs interface with management stations. As a result, proprietary (manufacturer-specific) protocols were

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

developed. The resulting RSUs and RSU systems are not interchangeable or interoperable, and that can seriously limit the seamless operations along an arterial corridor across multiple jurisdictions. If an agency wishes to use either a central management system or additional RSUs from a different manufacturer, the agency encounters significant systems integration challenges, requiring additional resources to address. These additional resource requirements inhibit information sharing within and between various potential users of the data and prevent manufacturer interoperability from a common remote monitoring and management platform/system. Without manufacturer interoperability, resource requirements further increase because of a lack of a competitive market.

Such challenges are not unique to RSUs. Many other roadway devices, such as traffic signal controllers, dynamic message signs, bus priority sensors, weather and environmental monitoring, and others, also need to exchange information with management systems.

To address these challenges, NTCIP is a family of open standards for communications between field devices and central management systems. NTCIP 1218 v01 is part of that larger family and defines an interoperable and interchangeable interface between a transportation management system and an RSU, while still allowing for extensions beyond NTCIP 1218 v01 to allow for new functions as needed. This approach is expected to support the deployment of RSUs from one or more manufacturers in a consistent and resource-efficient way.

NTCIP 1218 v01 standardizes the communications interface by identifying operational needs of the users (Section 2) and subsequently identifying the necessary requirements (Section 3) that support each need. NTCIP 1218 v01 then defines the NTCIP standardized communications interface used to fulfill these requirements by identifying the dialogs (Section 4) and related data concepts (Section 5) that support each requirement. Traceability among the various sections is defined by the Protocol Requirements List (Section 3.3) and the Requirements Traceability Matrix (Annex A). Conformance requirements for NTCIP 1218 v01 are provided in Section 3.3. NTCIP 1218 v01 only addresses a subset of the requirements needed for procurement.

NTCIP 1218 v01 does not address requirements related to the performance of the V2X radio, hardware components, mounting details, etc. NTCIP 1218 v01 also does not address requirements that relate to configure or manage applications that run on the RSU.

1.2 References

1.2.1 Normative References

Normative references contain provisions that, through reference in this text, constitute provisions of NTCIP 1218 v01. Other references in NTCIP 1218 v01 might provide a complete understanding or provide additional information. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on NTCIP 1218 v01 are encouraged to investigate the possibility of applying the most recent editions of the standards listed.

Identifier	Title
3GPP TS 23.285	Architecture Enhancements for V2X Services, 3GPP
IEEE 802.11-2016	IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (IEEE802dot11-MIB in Annex A.3)
IEEE 1609.2-2016	IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages, IEEE, 2016.
IEEE 1609.3-2016	IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services, IEEE, 2016.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

Identifier	Title
IEEE 1609.4-2016	IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation, IEEE, 2016.
IEEE 1609.12-2016	IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Identifier Allocations, IEEE, 2016.
IEEE Provider Service Identified (PSID) Registration Authority	IEEE Provider Service Identified (PSID) Registration Authority Note: See https://standards.ieee.org/products-services/regauth/psid/public.html
Libpcap	libpcap v1.9.0 Note: See https://www.tcpdump.org/
UCD-SNMP	UCD-SNMP-MIB.txt - University of California, Davis - ucdavis module, Last updated 200901190000Z. (UCD-SNMP in Annex A.3)
NIST FIPS PUB 180-4	Federal Information Processing Standards Publication 180-4, Secure Hash Standard, National Institute of Standards and Technology (NIST), August 2015.
NIST FIPS PUB 197	Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology (NIST), November 26, 2001.
NTCIP 1103 v03	Transportation Management Protocols (TMP), AASHTO / ITE / NEMA, published December 2016.
NTCIP 1201 v03	Global Object (GO) Definitions, AASHTO / ITE / NEMA, published March 2011. Note: Referred to as '1201v03' in Annex A.3.)
NTCIP 2103 v02	Point-to-Point Protocol over RS-232 Subnetwork Profile, AASHTO / ITE / NEMA, published December 2008. Note: Referred to as 2103v02 in Annex A.3.
RFC 2578	Structure of Management Information Version 2 (SMIv2), Internet Engineering Task Force (IETF), April 1999.
RFC 2579	Textual Conventions for SMIv2 (IETF). April 1999.
RFC 2580	Conformance Statement for SMIv2, Internet Engineering Task Force (IETF), April 1999.
RFC 3164	The BSD syslog Protocol (IETF), August 2001.
RFC 3413	Simple Network Management Protocol Applications, Internet Engineering Task Force (IETF), December 2002.
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), Internet Engineering Task Force (IETF), December 2002.
RFC 3416	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP), Internet Engineering Task Force (IETF), December 2002.
RFC 3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), Internet Engineering Task Force (IETF), December 2002.
RFC 3635	Definitions of Managed Objects for the Ethernet-like Interface Types, Internet Engineering Task Force (IETF), September 2003.
RFC 5424	The Syslog Protocol, Internet Engineering Task Force (IETF), March 2009.
RFC 5590	Transport Subsystem for the Simple Network Management Protocol (SNMP), Internet Engineering Task Force (IETF), June 2009.
RFC 5591	Transport Security Model for the Simple Network Management Protocol (SNMP), Internet Engineering Task Force (IETF), June 2009.
RFC 6347	Datagram Transport Layer Security Version 1.2, Internet Engineering Task Force (IETF), January 2012.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

Identifier	Title
RFC 6353	Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP), Internet Engineering Task Force (IETF), July 2011.
RFC 7860	HMAC-SHA-2 Authentication Protocols in User-Based Security Model (USM) for SNMPv3, Internet Engineering Task Force (IETF), April 2016.
SAE J2735_201603 MIB	Dedicated Short Range Communications (DSRC) Message Set Dictionary™, SAE
SAE J2945_201712	On-Board System Requirements for V2V Safety Communications

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 1218 v01. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on NTCIP 1218 v01 are encouraged to investigate the possibility of applying the most recent editions of the standard listed.

Identifier	Title
U.S. Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT)	Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT), USDOT
FHWA-JPO-17-589	DSRC Roadside Unit (RSU) Specifications Document v4.1, USDOT, Saxton Transportation Operations Laboratory, published April 28, 2017 Note: Referred to as RSU 4.1 Spec throughout.
NIST FIPS 186-4	Federal Information Processing Standards - Digital Signature Standard (DSS), National Institute of Standards and Technology, July 2013.
IEEE 1609.0-2013	IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture, IEEE, 2013.
ISO/TS 21177:2019	Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices
NIST SP 800-53 Rev. 5 (Draft)	Security and Privacy Controls for Information Systems and Organizations Note: This document is undergoing review.
NCCIC Alert TA17-156A	TA17-156A Reducing the Risk of SNMP Abuse, National Cybersecurity and Communications Integration Center, https://www.us-cert.gov/ncas/alerts/TA17-156A, June 5, 2017.
NTCIP 2202:2001	Internet (TCP/IP and UDP/IP) Transport Profile, AASHTO / ITE / NEMA, published December 2001. Note: Referred to as UDP or TCP throughout.
NTCIP 8004 v02	Structure and Identification of Management Information (SMI) , AASHTO / ITE / NEMA, published June 2010.
OMG Unified Modeling Language Specification, Version 1.5	OMG Unified Modeling Language Specification, Object Management Group, 2003 Note: Also see *State-Transition Diagrams: Testing UML Models, Part 4*, Copeland, Lee at https://www.stickyminds.com/article/state-transition-diagrams)

 © 2020 AASHTO / ITE / NEMA

1.2.3 Contact Information

1.2.3.1 Internet Documents

Obtain Request for Comment (RFC) electronic documents from several repositories online at:

www.rfc-editor.org
www.rfc-editor.org/repositories.html
for FTP sites, read ftp://ftp.isi.edu/in-notes/rfc-retrieval.txt

1.2.3.2 Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT)

The Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) may be viewed online at:

http://local.iteris.com/arc-it/

ARC-IT is the US ITS reference architecture and includes all content from the (now deprecated) National ITS Architecture v7.1 and the Connected Vehicle Reference Implementation Architecture (CVRIA) v2.2.

1.2.3.3 FHWA Documents

U.S. Department of Transportation Federal Highway Administration (FHWA) documents (with designations FHWA-JPO-…) are available at the U.S. Department of Transportation National Transportation Library, Repository & Open Science Access Portal (ROSA P):

https://rosap.ntl.bts.gov/

1.2.3.4 IEEE Standards

IEEE standards can be purchased on-line in electronic format or printed copy from:

Techstreet
6300 Interfirst Dr.
Ann Arbor, MI 48108
(800) 699-9277
www.techstreet.com/ieee

1.2.3.5 ISO, IEC, and ISO/IEC Standards

ISO, IEC, and ISO/IEC standards can be purchased on-line in electronic format or printed copy from:

Techstreet
6300 Interfirst Dr.
Ann Arbor, MI 48108
(800) 699-9277
www.techstreet.com

1.2.3.6 Libpcap Documents

Libpcap documents are available at:

https://www.tcpdump.org/

1.2.3.7 NTCIP Standards

Copies of NTCIP standards may be obtained from:

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

NTCIP Coordinator
National Electrical Manufacturers Association
1300 N.17th Street, Suite 900
Rosslyn, Virginia 22209-3801
www.ntcip.org
e-mail: ntcip@nema.org

1.2.3.8 Object Management Group Documents

Copies of OMG standards may be obtained electronically from the Object Management Group at:

www.omg.org

1.2.3.9 SAE International Documents

Copies of SAE International documents may be obtained from:

SAE International
400 Commonwealth Drive
Warrendale, PA 15096
www.sae.org

1.2.3.10 3GPP Documents

Copies of 3GPP documents may be obtained electronically from:

http://www.3gpp.org/

1.3 General Statements

<In the opinion of the responsible NTCIP working group, Section 1.3 does not apply in the context of NTCIP 1218 v01.>

1.4 Terms

For the purposes of NTCIP 1218 v01, the following terms, definitions, acronyms, and abbreviations apply. Electrical and electronic terms not defined here are used in accordance with their definitions in IEEE Std 100-2000. English words not defined here or in IEEE Std 100-2000 are used in accordance with their definitions in Webster's New Collegiate Dictionary.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

Term	Definition
Connected Device	A mobile device, such as a vehicle, smartphone or infrastructure safety device, equipped to transmit or receive data using Dedicated Short-Range Communications (DSRC)/ IEEE 802.11, 3GPP or other wireless communications.
Coordinated Universal Time (UTC)	UTC is the time standard commonly used across the world. The world's timing centers have agreed to keep their time scales closely synchronized – or coordinated. This 24-hour time standard is kept using highly precise atomic clocks combined with the Earth's rotation. UTC is similar to Greenwich Mean Time, but while UTC is a time standard, GMT refers to a time zone (similar to Eastern Standard Time). UTC never changes to account for daylight savings time. Note: UTC may have different references. RSU 4.1 Spec is based on 1/1/1970 while IEEE 1609.2 security is based on 1/1/2004 and needs to adjust for leap-year seconds.
Dedicated Short Range Communications	A V2X communications interface compliant with IEEE 802.11p.
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).
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. Note: From IEEE Standard Glossary of Software Engineering Terminology.
Management Station	The computer system with which the device communicates. Typically, the management station commands and monitors the device.
On-Board Unit (OBU)	A mobile device used to wirelessly communicate with other devices for safety and mobility purposes. Typically installed in a vehicle but may be on a pedestrian or a work zone worker.
PC5	A V2X communications interface compliant with 3GPP R14 PC5 mode 4.
Provider Service Identifiers	A globally unique integer value that is associated with a service being provided using a communications system such as 5.9 GHz WAVE. Source: IEEE 1609.12-2016
Roadside Unit (RSU)	Devices that serve as the demarcation component between vehicles and other mobile devices and existing traffic equipment. Note: From RSU 4.1 Spec. Also referenced as Connected Vehicle Roadside Equipment (CV RSE) in ARC-IT.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

Term	Definition
V2X Interface	A logical component of the RSU representing the wireless interface between the RSU and connected devices, such as connected vehicles. Note: While RSU connection to roadway users is wireless, some RSUs may connect to infrastructure via wire.

1.5 Abbreviations

The abbreviations and acronyms used in NTCIP 1218 v01 are defined as follows:

3GPP	Third Generation Partnership Project
ARC-IT	Architecture Reference for Cooperative and Intelligent Transportation
C-ITS	Cooperative Intelligent Transport Systems
CPU	Central Processing Unit
CVRE	Connected Vehicles Roadside Equipment
CVRIA	Connected Vehicles Reference Implementation Architecture
DTLS	Datagram Transportation Layer Security
DNS	Domain Name System
DSRC	Dedicated Short Range Communications
EDCA	Enhanced Distributed Channel Access
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GNSS	Global Navigation Satellite System
Hz	Hertz
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITS	Intelligent Transportation Systems
MAC	Media Access Control
MIB	Management Information Base
NTP	Network Time Protocol
OID	Object Identifier
PC5	ProSe Communications 5
PRL	Protocol Requirements List
PSID	Provider Service Identifier
RCPI	Received Channel Power Indicator

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

RF	Radio Frequencies
RFC	Request For Comments
RSE	Roadside Equipment (See Roadside Unit in Section 1.4 Terms)
RSSI	Received Signal Strength Indication
RTCM	Radio Technical Commission for Maritime Services
RTM	Requirements Traceability Matrix
SCMS	Security Credential Management System
SCP	Secure Copy Protocol
SNMP	Simple Network Management Protocol
SPaT	Signal Phase and Timing
TMC	Traffic Management Center
URL	Uniform Resource Locator
UTC	Coordinated Universal Time (also called “Common Universal Time”)
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
WAAS	Wide Area Augmentation System
WAVE	Wireless Access in Vehicular Environments
WG	Working Group
WGS	World Geodetic System
WRA	WAVE Router Advertisement
WSA	WAVE Service Advertisement
WSMP	WAVE Short Message Protocol

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

Section 2
Concept of Operations [Normative]

Section 2 defines the user needs that subsequent sections within NTCIP 1218 v01 address. Accepted system engineering processes detail that requirements should only be developed to fulfill well-defined user needs. The first stage in this process is to identify the ways in which the system is intended to be used. In the case of NTCIP 1218 v01, this entails identifying the various ways in which transportation managers or transportation operators may use RSU information to fulfill their duties.

This concept of operations provides the reader with:

a) a detailed description of the scope of NTCIP 1218 v01;
b) an explanation of how an RSU is expected to fit into the larger context of an ITS network;
c) a starting point in the agency procurement process; and
d) an understanding of the perspective of the designers of NTCIP 1218 v01.

Section 2 is intended for all readers and users of NTCIP 1218 v01, including:

a) **Transportation Managers:** Agency personnel responsible for making decisions about operational strategies to implement and configuring transportation field devices.
b) **Transportation Operators:** Agency personnel responsible for monitoring the transportation infrastructure and implementing transportation strategies.
c) **Transportation Engineers:** Agency personnel responsible for planning or designing the transportation infrastructure.
d) **Maintenance Personnel:** Agency personnel responsible for ensuring that transportation field devices operate as intended.
e) **System Integrators:** Entities that brings together different components or subsystems into a whole system that functions together.
f) **Device Manufacturers:** Vendors providing transportation field devices. May also include vendors providing central systems to configure, monitor and control these field devices.
g) **Application Developers:** Vendors providing applications that run on transportation field devices or custom applications that run from a central server, cloud service, or back-office location.

For the first four categories of readers, Section 2 is useful to understand how RSU equipment can be used in their system. For this audience, Section 2 serves as the starting point in the procurement process and enables these readers to become familiar with each feature supported by NTCIP 1218 v01 and determine whether that feature is appropriate for their implementation. If appropriate, then the procurement specification needs to require support for the feature and all mandatory requirements related to that feature.

For the last three categories of readers, Section 2 provides a more thorough understanding as to why the more detailed requirements exist later in NTCIP 1218 v01.

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 system developers understand users' needs. Within the context of NTCIP standards, a concept of operations documents the intent of each feature for which NTCIP 1218 v01 supports a communications interface. It also serves as the starting point for users to select which features may be appropriate for their project.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

The concept of operations starts with a discussion of the current situation and issues that have led to the need to deploy systems covered by the scope of NTCIP 1218 v01 and to the development of NTCIP 1218 v01 itself. This discussion is 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:

a) **Reference Physical Architecture:** The reference physical architecture (view) defines the overall context of the proposed system and defines which specific interfaces are addressed by NTCIP 1218 v01. The reference physical architecture is supplemented with one or more samples that describe how the reference physical architecture may be realized in an actual deployment.
b) **Architectural Needs:** The architectural needs section discusses the issues and needs relative to the system architecture that have a direct impact on NTCIP 1218 v01.
c) **Features:** The features identify and describe the various functions that users may want components of an RSU system to perform. These features are derived from the high level user needs identified in the problem statement (Section 2.2) but are refined and organized into a more manageable structure that forms the basis of the traceability tables contained in Section 3 and Annex A.

The architectural needs and features are collectively called user needs. Section 3 uses these user needs in the analysis of the system to define the various functional requirements of an RSU. Each user need traces to one or more functional requirements, and each functional requirement is derived from at least one user need. This traceability is shown in the Protocol Requirements List (PRL) in Section 3.3.

While NTCIP 1218 v01 is intended to standardize communications across a wide range of deployments, it is not intended to mandate support for every feature for every deployment. Therefore, the PRL also defines each user need and requirement as mandatory, optional, or conditional. The only items marked mandatory are those that relate to the most basic functionality of a roadside unit. To procure a roadside unit that meets specific needs, the user first identifies which optional needs are necessary for the specific project.

Each requirement identified is then presented in the Requirements Traceability Matrix (RTM) in Annex A, which defines how the requirement is fulfilled through standardized dialogs and data element definitions provided in Section 4 and Section 5.

A conformant device may support other user needs, as long as these are conformant with the requirements of NTCIP 1218 v01 and its normative references (see Section 1.2.1). For example, a device may support data that has not been defined by NTCIP 1218 v01; however, when exchanged via an SNMP-like protocol, the data shall 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 inhibits the goals of interoperability and interchangeability, especially if the documentation of these user needs is not available for distribution to system integrators. NTCIP 1218 v01 allows implementations to support additional user needs 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 concept of operations concludes by describing the security needs for NTCIP 1218 v01 and by providing a description of how NTCIP 1218 v01 relates to the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) (formerly the National ITS Architecture and the Connected Vehicle Reference Implementation Architecture).

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

2.2 Current Situation and Problem Statement [Informative]

The Cooperative-ITS (C-ITS) environment, also known as connected vehicles, started as a research program led by USDOT to investigate how transportation connectivity potentially enables applications to improve the US's transportation system in the areas of safety, mobility and the environment. Transportation connectivity can take place between vehicles (vehicle-to-vehicle, V2V) to enable crash prevention; between vehicles and the infrastructure (vehicle-to-infrastructure, V2I) to enable additional safety, mobility and environmental benefits; between personal devices and the infrastructure (personal-to-infrastructure, P2I) to enable safety and mobility benefits; and among vehicles, infrastructure and personal devices (vehicle-to-everything, V2X) to provide continuous real-time connectivity.

The RSU is a key component of the C-ITS environment. The RSU provides an interface: 1) between a traffic management center (TMC) and a connected device (including connected vehicles); and 2) between connected devices and other ITS roadside devices (e.g., a traffic signal controller) through a managed network. The RSU allows transportation managers to exchange information between connected devices and the infrastructure (traffic management centers and ITS roadside devices), collecting data from one component and forwarding that same data to another component. Through this data exchange, managers and applications can use this data to:

a) Improve surface transportation safety by better controlling traffic operations on the roadway and providing directed warnings to travelers;
b) Improve mobility by optimizing traffic operations and through warnings and advisories to travelers; and/or
c) Improve the environment by more efficiently managing traffic operations to reduce delays, fuel consumption and emissions.

While a number of standards define V2V and V2I interfaces, prior to NTCIP 1218 v01, no standard defines the center to RSU interface. As the C-ITS environment is deployed, it becomes increasingly important to develop a standard to interface with and manage the RSU from a TMC instead of using proprietary communications protocols.

The lack of such a standard results in several RSU deployment challenges. Device interoperability and consistent device monitoring and management are examples of such challenges. Despite the development of an RSU 4.1 Spec sponsored by USDOT, the RSU 4.1 Spec has not been implemented consistently for conformance, therefore not guaranteeing interoperability. The RSU 4.1 Spec also provides no guidance for extensions to support needed capabilities (beyond those functions defined in RSU 4.1 Spec).

Comparing existing RSU deployments, different architectures have been designed for the RSU system, and different standards or methods have been used for exchanging data, such as uploading applications, across the center and RSU interface.

These inconsistent deployments create barriers for transportation managers at agencies to easily deploy and manage RSU devices.

2.3 Reference Physical Architecture [Informative]

Section 2.3 represents an overview of what a complete RSU system may look like for a transportation agency, and identifies the specific information exchange paths to be addressed by NTCIP 1218 v01 and related standards. Figure 1 presents a graphical depiction of the physical architecture around an RSU system.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

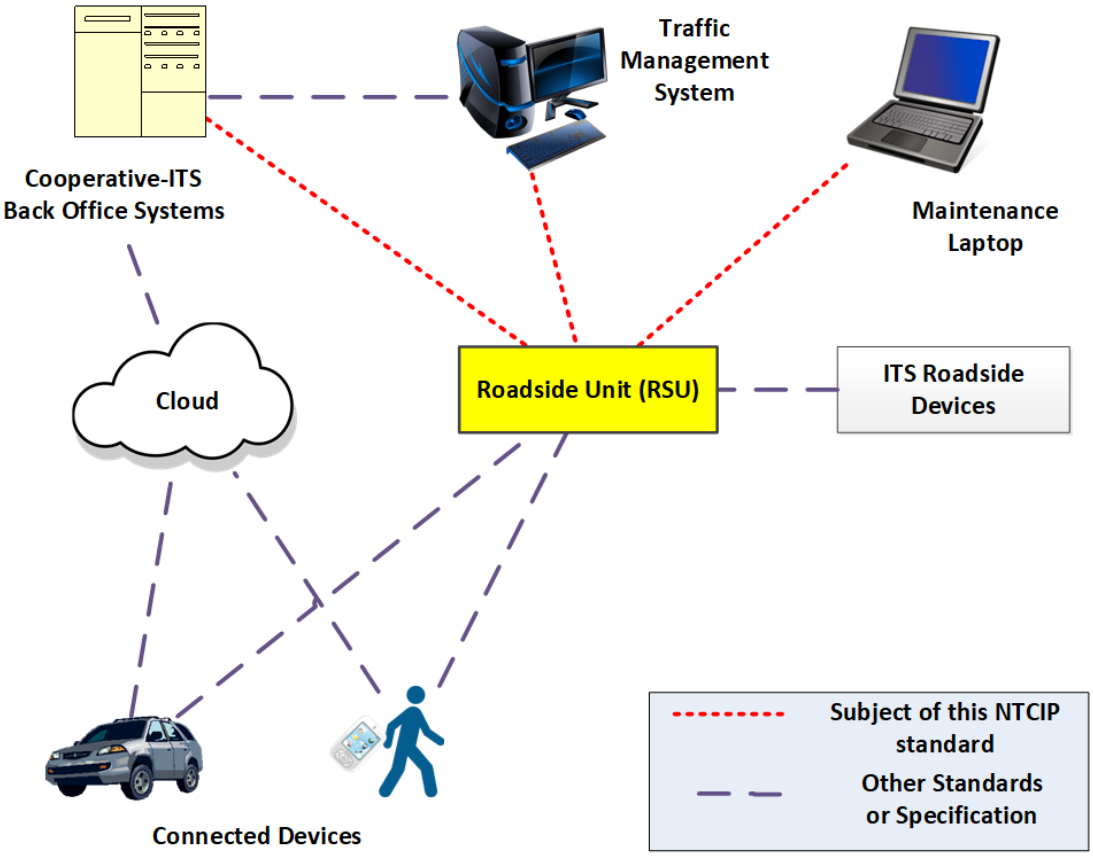

Figure 1 Reference Physical Architecture: RSU System

The RSU system is a collection of devices, including:

a) **Roadside Unit (RSU):** A field device that supports secure communications with connected devices, and may include a computing platform running applications. The RSU exchanges data among nearby connected devices (vehicles or mobile devices), other ITS Roadside Devices, and management systems at centers (such as a Traffic Management Center (TMC) or a Connected Vehicle Back Office System). In this context, the RSU is a NTCIP device.
b) **ITS Roadside Devices:** A host computing platform that may manage roadway control devices (such as a traffic signal controller) or collect and forward sensor data from roadway devices (such as roadway weather sensors or vehicle detectors).
c) **Traffic Management System:** A management station typically located in some type of management center (e.g., a Traffic Management Center) and may be physically located at a considerable distance away from the RSU. A management station in this context is a host computing platform that manages one or more NTCIP field devices, such as an RSU. The management station is responsible for configuring, monitoring, and controlling the RSU. There may be multiple management stations for a given RSU. A “manager” is a transportation system manager (or maintenance personnel), who needs to access information in the RSU through the management station.
d) **Maintenance Laptop:** A computer that maintenance personnel (such as a field technician) may use on a trip to visit the RSU or a field processor that may be used to access the RSU. It typically acts as an on-site management station for the RSU, capable of configuring, monitoring, and controlling the RSU. It typically plugs directly into the RSU and is commonly used to monitor the data reported from the RSU.
e) **Connected Devices:** A mobile device, such as a vehicle with an OBU, smartphone, or infrastructure, equipped to exchange data using wireless communications.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

f) **Cooperative-ITS (C-ITS) Back Office Systems:** Represent computer systems that supports the C-ITS environment, including security services.
g) **Cloud:** A connection (typically wireless) between the mobile devices and the Cooperative-ITS Back Office Systems for exchanging data.

2.3.1 RSU Characteristics - General

NTCIP 1218 v01 addresses the communications interface between a management station and an RSU. USDOT's RSU 4.1 Spec defines:

> "The purpose of the RSU is to facilitate communication between transportation infrastructure and vehicles and other mobile devices by exchanging data over DSRC in compliance with industry standards, including but not limited to (IEEE 802.11, IEEE 1609.x, SAE J2735, and SAE J2945). Additionally, the RSU can be integrated with a backhaul system to enable remote management and provide vehicles and other mobile devices with services and applications delivered by back office service providers."

The United States Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) also implies a logical framework of applications and services that are allocated to the RSU. Based on these definitions and through discussions with stakeholders, an RSU system can be viewed as three logical components, as shown by the blue circles in Figure 2.

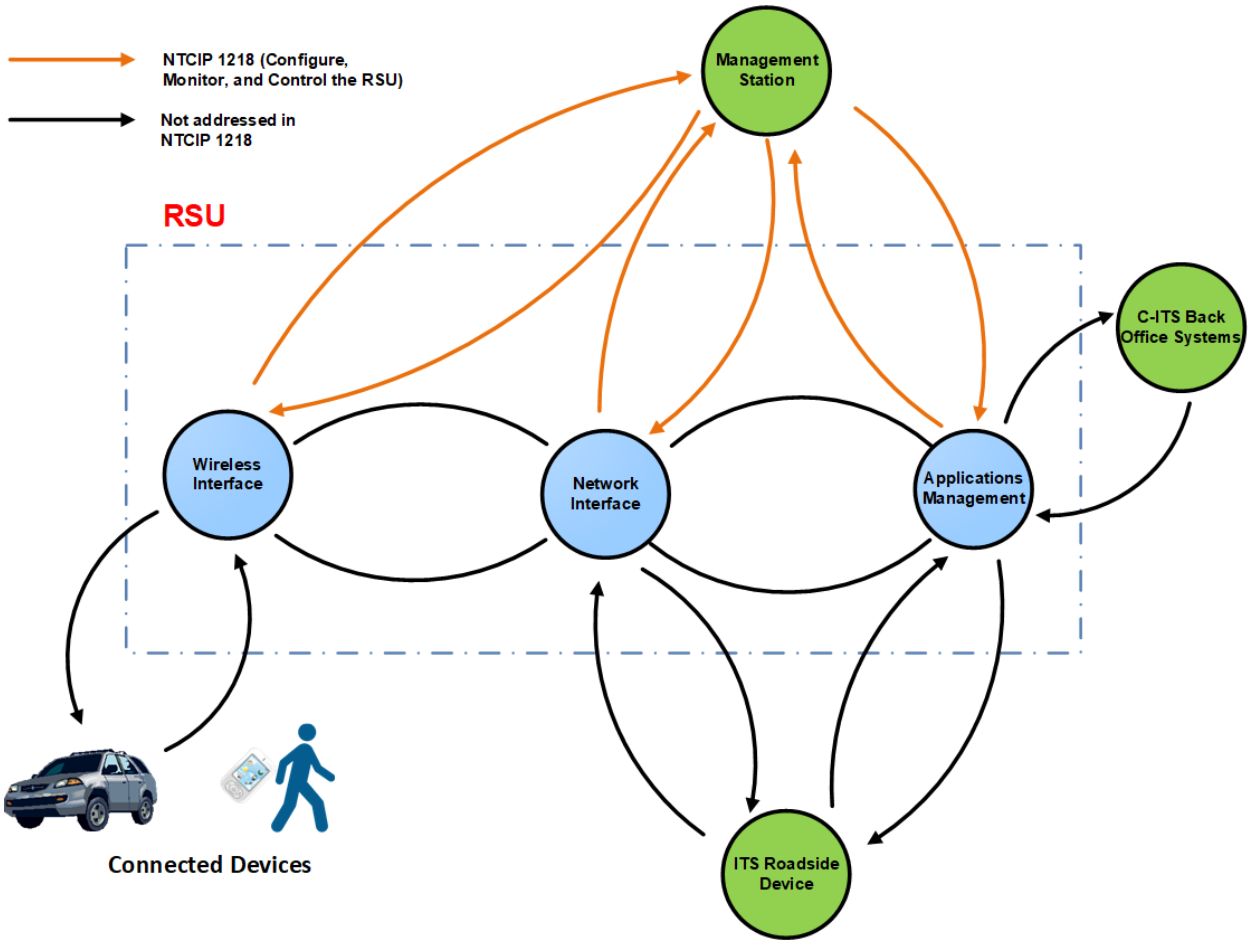

Figure 2 RSU Context Diagram

© 2020 AASHTO / ITE / NEMA

The first component is the V2X Interface, which is the wireless interface for communicating with vehicles and connected devices. Although the RSU 4.1 Spec assumes the wireless radio to conform to standards such as IEEE 802.11 and IEEE 1609.x standard, NTCIP 1218 v01 strives to be technology-neutral, although the primary focus is on and includes DSRC technology. This allows NTCIP 1218 v01 to support potential future wireless technologies while maintaining support for the other components of an RSU.

The second component is the Network Interface. The RSU serves as a demarcation component among vehicles and other connected devices through the V2X interface, other ITS roadside devices (such as traffic signal controllers, environmental sensor stations, or dynamic message signs), and center systems such as a traffic management system. As a network interface, the RSU facilitates communications among these devices and systems.

The third component is the Applications Management, where the RSU serves as a computing platform for applications that provide services to travelers, infrastructure owner-operators, or other users in a C-ITS environment. This component uses inputs (from vehicles, connected devices, ITS roadside devices or traffic management systems) to provide these services. The Applications Management also enable the security features, available from the C-ITS Back Office Systems for the RSU.

Figure 2 also depicts the interfaces between the different components and devices that comprise the C-ITS environment around and including the RSU. The interface between the management station and the V2X Interface, and the interface between the management station and the Network Interface are solid orange lines, which indicates these interfaces are addressed by NTCIP 1218 v01 and the NTCIP family of standards. Only RSU configuration, monitoring, and control data are addressed by NTCIP 1218 v01. Management of other data, such as applications data beyond the operational environment of the RSU, is not in scope. Applications data include software applications or data collected and stored by software applications. The management station may be a traffic management system or a maintenance laptop.

The remaining interfaces are in black and are outside the scope of NTCIP 1218 v01, although the data across those interfaces should be defined by one or more standards or an industry specification.

From a physical point of view, two possible physical architectures are considered in NTCIP 1218 v01, defined by where the Applications Management component is physically located. In the first architecture (Figure 2), the Applications Management is physically located within the same device as the Network Interface and the V2X Interface. In the second architecture (Figure 3), the Applications Management, shown in maroon, is physically located in a separate computing device apart from the device with the Network Interface and V2X Interface. The Applications Management can, for example, be physically located within the management station or the ITS Roadside Device.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

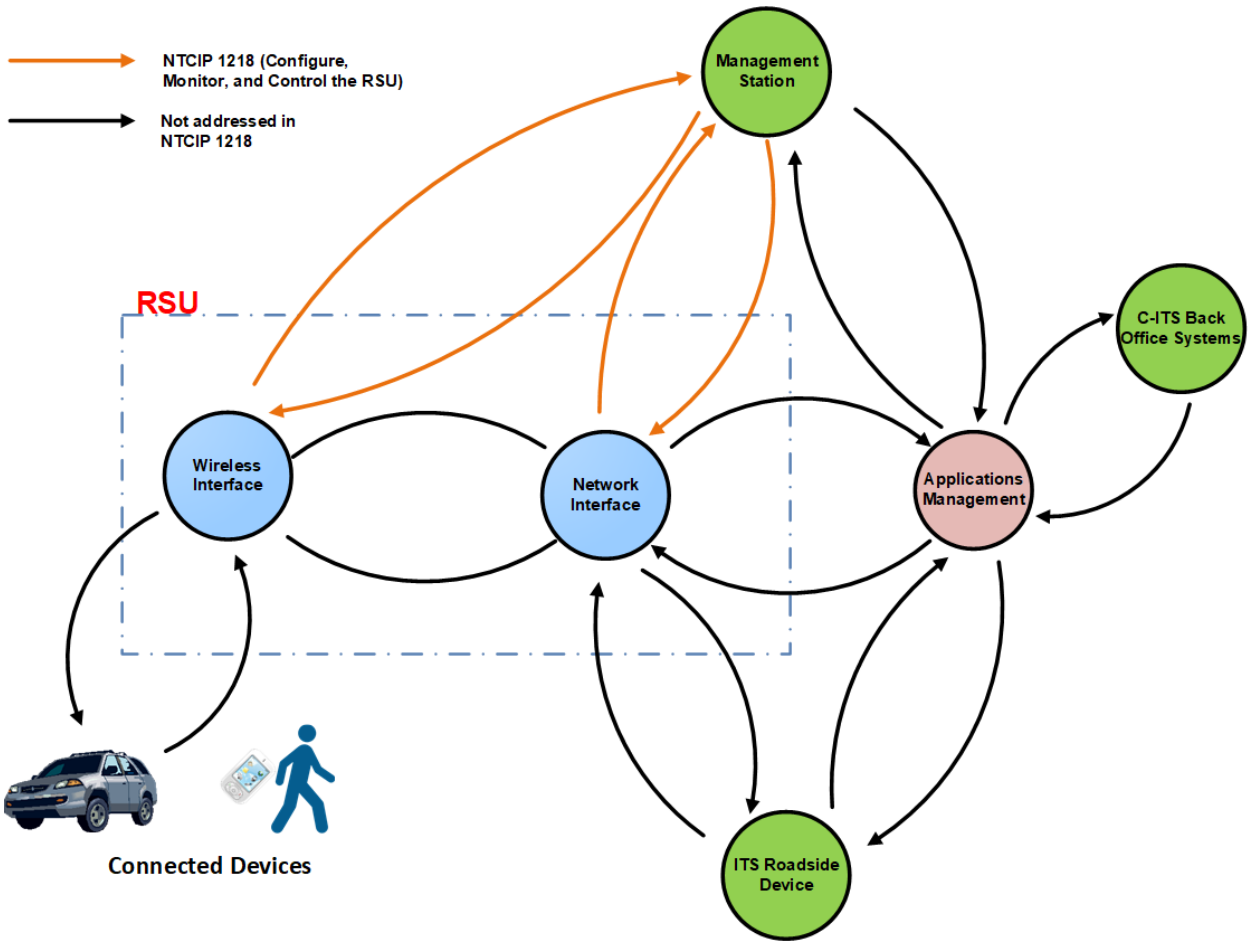

Figure 3 RSU Alternate Context Diagram

It is also possible that the V2X Interface and Network Interface are located in separate physical boxes, but that is not relevant in NTCIP 1218 v01.

2.3.2 RSU Characteristics - V2X Radio Type

The previous section describes the first logical component that NTCIP 1218 v01 is intended to address as the V2X Interface, which is the wireless interface for communicating with vehicles and connected devices. Although NTCIP 1218 v01 strives to be technology-neutral, some requirements apply to specific communications technologies. The technologies addressed in NTCIP 1218 v01 are:

a) **DSRC Radio:** Defined by IEEE 802.11 and the Federal Communications Commission.
b) **PC5 Radio:** Defined in 3GPP Release 15 (See 3GPP TS 23.285), PC5 is an interface for short range communications between devices.

2.4 Architectural Needs

NTCIP 1218 v01 addresses the interface between an RSU and one or more management stations (e.g., central computers, laptops, etc.). The management station may also need to retrieve data that has been collected by the RSU, and manage applications on the RSU. After the management station has retrieved the data of interest, a manager can use the retrieved data to make decisions and initiate other events (such as changes to the traveler information messages) to better manage the transportation system.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

To fulfill these needs, the transportation system manager needs to establish a communication system that links the RSU with a management station. For some systems, the resources required for communications may be minimal; other systems may require significant resources for communicating with the RSU and as such the system may be designed to minimize data exchanges. When deploying an RSU, the system designer needs to consider which of the following operational environments need to be supported.

The RSU acts as an intermediary between the management station and the connected devices, such as OBUs. The RSU provides support functions in that role, such as firmware updates, data retrieval, and process management. The RSU also needs to support the exchange of data from connected devices for road network monitoring, safety, and other applications.

An RSU is expected to operate in the communications environment defined as follows.

2.4.1 Configure, Monitor and Control the RSU

A transportation manager and transportation operator need to retrieve data and control the RSU by issuing requests (e.g., requests to access information, alter information, or control the device). In this environment, the RSU responds to requests from the management station (e.g., through the provision of live data, success/failure notice of information alteration, or success/failure of the command).

2.4.2 Provide for Log Data Local Storage and Retrieval

In a typical operational environment, a transportation operator needs logged data from the RSU for diagnostic purposes, and for operational environments (e.g., dial-up links) that do not have always-on connections. For example, logged data may include the time when the communications connectivity is broken.

2.4.3 Condition-based Exception Reporting

In some operational environments, a transportation operator needs to have the RSU automatically transmit data to the management station when certain conditions occur. Under this scenario, a transportation manager can program the information to be automatically reported to the management station when a specified condition occurs. An example is a manager wants to know when an RSU enclosure door is opened, a power failure is detected, or an attempt to potentially hijack the device is detected; these conditions can be programmed to cause the transmission of the alarm objects thus providing the management station with information regarding the change of state at the RSU cabinet.

2.5 Features

The features that may be offered by the RSU follow.

2.5.1 Manage the RSU Configuration

The features that allow a transportation manager to manage the configuration of the RSU follow.

2.5.1.1 Manage the RSU Device

The features that allow a transportation manager to manage the RSU device follow.

2.5.1.1.1 Retrieve RSU Identity

A transportation manager needs to request and obtain basic information about the RSU. This information consists of the make, model, and version of the device components. The device components can be a hardware, software, or firmware component, and could be a physical or logical entity in nature. This feature allows the manager to verify the identity of the RSU in the field and what software or firmware

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

version is installed. This feature also allows the manager to retrieve a unique identifier of the RSU as provided by the RSU manufacturer, and the version of standards supported by the RSU.

2.5.1.1.2 Retrieve Configuration Version of the RSU

A transportation manager needs to determine the version of the configuration parameters for the RSU. This feature allows a manager to determine if the RSU has the correct and expected values of the configuration parameters. The configuration version identifier changes whenever a value of a configurable parameter changes. For example, a manager can check the current version identifier of an RSU and if the value of the version identifier is different than expected by the manager, the difference indicates that configuration of the RSU has changed.

2.5.1.1.3 Manage RSU Location Information

A transportation manager needs to configure a RSU's location (latitude, longitude, and elevation) information. This feature allows a manager to manually enter the reference location of the RSU, use the location as reported by an external subsystem, and determine the legitimacy of the subsystem used. This feature also allows a manager to configure the location of the antenna for the V2X Interface. The location information may be used for security purposes or used to compare with the location data of the devices that are connected to the RSU.

2.5.1.1.4 Manage RSU Startup Functions

A transportation manager needs to retrieve and configure the startup capabilities and functions of the RSU. This feature allows the manager to retrieve and configure user-definable parameters; not the manufacturer-defined parameters.

2.5.1.1.5 Manage RSU Firmware Version

A transportation manager needs to manage the firmware version of the RSU. This feature allows the manager to locally or remotely install new firmware updates on the RSU.

2.5.1.1.6 Manage Communications Loss

A transportation manager needs to configure the functionality and behavior of an RSU when backhaul communications with the traffic management center is lost.

2.5.1.1.7 Manage Notifications

A transportation manager needs to configure the target network addresses and port number that an RSU transmits notifications to when a configured event occurs. This feature also allows a manager to assign a priority level to different notifications.

2.5.1.2 Manage Network Interface

The features that allow a transportation manager to manage network communications and data across the RSU follow.

2.5.1.2.1 Manage a Network Interface

A transportation manager needs to configure a network interface for an RSU. This feature consists of enabling or disabling the communications ports, configuring the port address (e.g., IP address), and configuring security, including access controls (e.g., which application entities are accessible from the physical port). Network interfaces might support one or more protocols, including IPv4, IPv6 or WSMP. This feature allows a manager to disable an unused communications port for security purposes or restrict access (e.g., to SNMP commands) from non-defined physical ports.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

2.5.1.2.2 Manage Messages

The features related to managing messages received and sent by the RSU follow. These features allow a manager to manage the data (or messages) received or sent by the RSU device. The actions defined by the manager upon receiving a message may be determined by the type of message or the network interface from which it is received.

2.5.1.2.2.1 Manage Stored Messages

A transportation manager needs to manage the messages stored on an RSU for transmission. Stored messages may be transmitted by the RSU during a configured time period. This feature allows a manager to view, edit, or delete stored messages. The stored message may already be signed.

2.5.1.2.2.2 Manage Stored Messages for Transmission

A transportation manager needs to configure the parameters of when a stored message on an RSU is transmitted. This feature allows a manager to configure the network destination, the rate, the time period, transport protocol, priority level and the communications channel the message is transmitted by the RSU. This feature also allows a manager to associate the message with a specific service, and if the message should be signed or encrypted when transmitted. Messages may be signed before being provided to the RSU for transmission.

2.5.1.2.2.3 Manage Received Messages for Forwarding to the V2X Interface

A transportation manager needs to configure an RSU to forward messages received on a specific port number to the V2X interface. The configuration may be based on the type of message. This feature allows a manager to configure the transport protocol, priority level and the communications channel the message is forwarded by the RSU. This feature also allows a manager to associate the message with a specific service, and if the message should be signed or encrypted when forwarded.

2.5.1.2.2.4 Manage Received Messages from the V2X Interface for Forwarding

A transportation manager needs to configure an RSU to forward messages received from the V2X interface to a specified network destination. The configuration may be based on the type of message or the receive signal strength. This feature allows a manager to configure the network destination and the transport protocol. The receive signal strength is used to filter messages by signal strength.

2.5.1.2.2.5 Manage Transmitted Messages over the V2X Interface for Forwarding

A transportation manager needs to configure an RSU to forward messages transmitted over the V2X interface to a specified network destination. This feature allows a transportation manager to view what messages are being transmitted by the RSU over the V2X interface without looking at the interface logs on the RSU. The configuration may be based on the type of message. This feature allows a manager to configure the network destination and the transport protocol.

2.5.1.2.3 Manage Logging of Interface Data

A transportation manager needs to configure an RSU to log interface data. The interface log is used to log data packets across a network interface on the RSU for later analysis for the purposes of integration and diagnostics. This feature allows a manager to configure which network interface, the direction of data packets, the maximum log file size allowed, the maximum collection time, start time, end time, and collection interval to be logged. Each interface log entry includes the date and time the data packet was logged, the contents of the data packet and the RF signal levels for network interfaces using wireless communications. This feature is available for any RSU interface.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

2.5.1.3 Configure V2X Interface

The features that allow a transportation manager to transmit and receive messages via a V2X interface follow.

2.5.1.3.1 Enable/Disable Radios

A transportation manager needs to enable and disable the radios controlled by the RSU. This feature allows the manager to enable and disable a radio when it is not used, either for security or to conserve energy.

2.5.1.3.2 Determine Lower Layer Parameters

A transportation manager needs to retrieve the Lower Layer parameters for supporting wireless communications across the V2X interface. The Lower Layer parameters may include parameters such as transmit power, transmission rate and communications channel. This is a data dictionary standard - the lower layers deal with the implementation of the data dictionary standard.

2.5.1.3.3 Configure IEEE 1609 Communications

The features for transmitting and receiving messages using IEEE 1609 communications follow.

2.5.1.3.3.1 Configure IEEE 1609.2 Security

A transportation manager needs to configure the IEEE 1609.2 security profile used by the RSU. The IEEE 1609.2 defines security processing requirements and certificates for secure communications.

2.5.1.3.3.2 Configure IEEE 1609.3 Communications - WSA

A transportation manager needs to configure an RSU to advertise available services using an IEEE 1609.3 WAVE service advertisement (WSA). This feature allows a manager to configure the advertisement to support one or more applications. WSA are typically broadcast to connected devices to indicate channel assignments, PSID, priority, transmission rate, transmit power, and WAVE router advertisements (WRA).

2.5.1.3.3.3 Configure IEEE 1609.4 Communications

A transportation manager needs to configure the RSU use of IEEE 1609.4 multi-channel operations. This feature allows a manager to configure the radio to operate in one of the available multi-channel operations modes.

2.5.1.3.3.4 Configure Radio Transmitter Properties

A transportation manager needs to configure the radio transmitter properties of the RSU. This feature stores information that is used for transmission power calculations.

2.5.1.4 Manage RSU Applications

The features that allow a transportation manager to manage the applications on an RSU follow.

2.5.1.4.1 Manage RSU Application

A transportation manager needs to manage the operational state of applications on the RSU. An RSU may have several software applications installed on the RSU to provide C-ITS services. This feature allows a manager to install, update or delete a software application residing on the RSU over the traffic management center to RSU interface. This feature also supports the transmission of the secure

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

installation files, including executable application code and associated support files to support executing an application on the RSU. The application code may not be interoperable for all RSUs.

2.5.1.4.2 Save and Restore Application Configuration

A transportation manager needs to save and restore an application configuration on the RSU. The configuration defines the parameters for the RSU. In the event of a failed update the RSU reverts to the last configuration prior to the update. This feature allows a manager to restore a configuration in the event the integrity of the data on the RSU is affected or a parameter on the RSU is changed and impacts the operation of the RSU.

2.5.1.5 Manage Location Corrections

A transportation manager needs to configure an RSU to compute and broadcast location correction data, such as RTCM, through the V2X interface. Location correction data can improve location accuracy. This feature allows a manager to identify the positioning corrections available and to configure the interval between broadcasts.

2.5.2 Monitor the RSU

The features that allow a transportation operator to monitor the processes and status of an RSU follow.

2.5.2.1 Determine RSU Operational Performance Status

A transportation operator needs to determine the operational performance of the RSU. This feature allows an operator to monitor the resources available on the RSU, such as the free memory available, the central processing unit (CPU) load (instantaneous, averaged over a period of time), the storage space available, the time elapsed since connectivity to the management center was restored, and the time elapsed since the RSU was operational or non-operational.

2.5.2.2 Determine Mode of Operations

A transportation operator needs to determine the current mode of operation of the RSU. This feature allows an operator to determine what functions and capabilities are currently enabled. The modes of operations are: fully operational, standby (non-transmit) mode, and fault.

2.5.2.3 Determine RSU Clock Status

A transportation operator needs to check the validity of an RSU system clock. The system clock is used to assign timestamps on messages broadcasted by the RSU. The primary system clock for the RSU is expected to be based on a trusted GNSS source, but may have a secondary source, such as NTP. This feature allows an operator to view which clock source is currently active and to specify allowable tolerances for clock drifts. The system clock is also used to drive the scheduler.

2.5.2.4 Determine RSU Location

A transportation operator needs to monitor the location information available to and used by an RSU. The location identifies the position of the RSU. Errors may include communication errors between the RSU and its location subsystem source or if there are sudden changes with the location data. Sudden changes to the location data may indicate an attack on the RSU, either physically or a cyberattack. If the location source is a GNSS device, this feature also allows the operator to monitor the number of GNSS satellites the GNSS receiver is tracking. For security purposes, the RSU may need to determine if it is within a legitimate boundary. This feature also transmits alerts if the RSU location changes or if errors are detected.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

2.5.2.5 Monitor Network Interfaces

A transportation operator needs to monitor a network interface with the RSU. This feature allows an operator to retrieve network statistics and diagnostic information. The network interface includes the interface between the management station and the RSU.

2.5.2.6 Report Number of Messages Exchanged

A transportation operator needs to track the number of messages received and transmitted by the RSU for each interface. This can be used for diagnostics.

2.5.2.7 Determine Number of Active Radios

A transportation operator needs to monitor how many radios are active. This feature can be used to check the system status.

2.5.2.8 Determine RF Communications Range

A transportation operator needs to determine the communications range of the RSU. This feature allows an operator to determine the range of RF communications based on the position of the connected devices and how it might change with different weather conditions, interference conditions, foliage, construction, etc.

2.5.2.9 Determine Application Status

A transportation operator needs to monitor the status of the applications residing on the RSU. This feature allows an operator to determine what applications are currently running on the RSU.

2.5.2.10 Determine RSU Environment

A transportation operator needs to determine the operating environment of the RSU. This feature allows an operator to monitor for unsafe operating environments for the RSU so proper precautions can be taken. Unsafe operating environment includes excessive internal RSU temperatures.

2.5.2.11 Determine RSU Current Status

A transportation operator needs to determine the current overall status of the RSU. This feature allows an operator to determine if any conditions exist on the RSU that requires additional monitoring, or if the RSU requires maintenance.

2.5.3 Control the RSU

The features that allow a transportation operator to control the operation of an RSU follow.

2.5.3.1 Control Mode of Operation

A transportation operator needs to control the mode of operation of an RSU. The mode of operation defines the ability for the RSU to process and exchange information with other devices. The modes of operations an operator can command an RSU to include fully operational, and standby (non-transmit) mode.

2.5.3.2 Control RF Antenna Output

A transportation operator needs to configure the transmit output power for a radio of an RSU. This feature allows an operator to control the output power of a RF antenna, possibly to change the transmission area around the antenna in compliance with government (e.g., FCC) regulations. This is a default transmit

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

output power for the RSU. An application residing on the RSU may elect to use a different output power for a message.

2.5.3.3 Reboot RSU

A transportation operator needs to remotely reboot an RSU. This feature allows an operator to remotely (warm) reboot the RSU to attempt to recover from a software failure or other operational failures. This feature is desired to avoid a field trip to reboot the RSU.

2.5.3.4 Control Application

A transportation operator needs to remotely manage an application on the RSU. An RSU may have several applications installed on the RSU to provide C-ITS services. This feature allows an operator to enable/disable or restart an application residing on the RSU.

2.6 Security

The security features that may be offered by the RSU follow.

2.6.1 Manage Authentication

A transportation manager needs to manage the RSU to authenticate the management station that the RSU is exchanging data (transmitting to or receiving from). This feature allows a transportation manager to configure whether the management station that is monitoring or configuring the RSU is “trusted” and, therefore, unlikely to provide data that can adversely affect the cooperative-ITS system.

2.6.2 Manage Data Integrity

A transportation manager needs to configure the RSU to protect the integrity of the data exchanged and stored on it and to verify that the content of data is unchanged when received or stored. For data exchanges, that the data contents when transmitted are the same as when received; and are not corrupted and used for misbehavior.

2.6.3 Manage Availability

A transportation manager needs to configure the RSU so that the RSU and its data are available to authorized users and processes. This feature allows a transportation manager to configure the RSU to permit appropriate processes and users timely and reliable access to the RSU.

2.6.4 Manage Confidentiality

A transportation manager needs to configure the RSU to protect the data exchanged with the RSU from unauthorized viewing. This feature protects the data from being used by hostile parties to attack the cooperative-ITS infrastructure.

2.7 Operational Policies and Constraints

The NTCIP 1218 v01 assumes that the following constraints apply.

a) Agencies have operational policies in place that limit physical access to authorized personnel and remote access to authorized personnel. It is recommended that the operational policies require each manager and operator be individually identified when accessing the RSU, and thus, each manager and operator should have their own username.
b) It is the operational policy of some agencies that authorized personnel is/are present at the physical location of the RSU, before an RSU accepts a change to the configuration of the RSU.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

c) Protocols defining communications to the RSU are limited to protocols already defined in another standard or RFC.
d) Agencies may also have policies and practices that limit the hours of operation of transportation managers and operators. RSU may need to be scheduled for operation.
e) NTCIP 1218 v01 defines a MIB and requires a compatible communications protocol.
f) At the time NTCIP 1218 v01 was developed, the RSU 4.1 Spec exists, but there is not yet an RSU standard.

2.8 Relationship to the ITS National Architecture [Informative]

Architecture Reference for Cooperative and Intelligent Transportation, known as ARC-IT, combines the National ITS Architecture and the Connected Vehicle Reference Implementation Architecture (CVRIA). Figure 1 is a Systems Engineering Tool for Intelligent Transportation (SET-IT) diagram representing instances of physical objects from ARC-IT as applied to NTCIP 1218 v01.

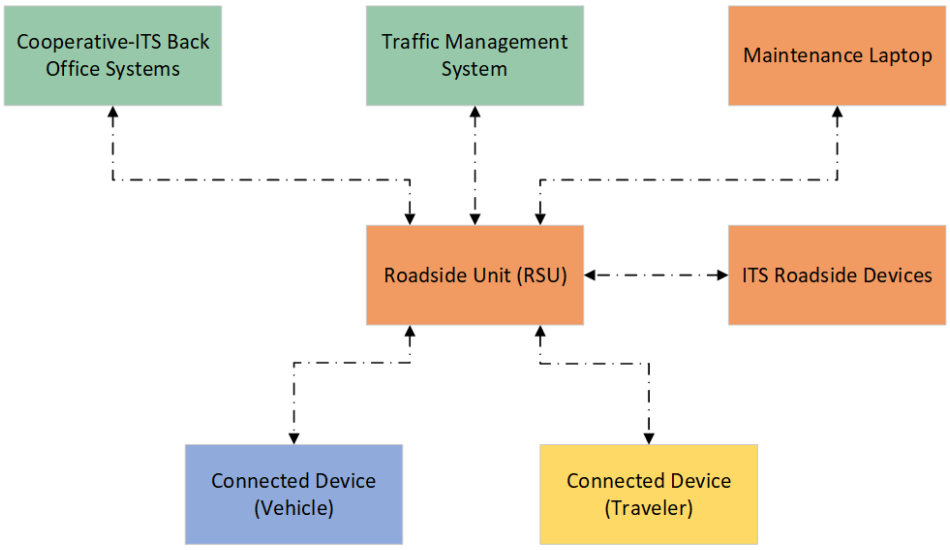

Figure 4 SET-IT Diagram for NTCIP 1218 v01

ARC-IT identifies a set of information flows that interface between an RSU, represented in ARC-IT as Connected Vehicle Roadside Equipment (CVRE), and other entities, including a center (CEN), Field Maintenance Equipment (FME), and Service Monitor System (SMS). As a subset of these flows, only flows not specific to individual ITS applications are addressed by NTCIP 1218 v01 as they represent the configuration, monitoring, and control of Connected Vehicle Roadside Equipment. These information flows are:

a) **Device Identification.** An identifier and device type designation that is used to uniquely identify a device in the Connected Vehicle Environment.
b) **Equipment Control Commands.** System-level control commands issued to the RSE such as reset and remote diagnostics.
c) **RSE Application Information.** RSE application configuration data and parameters that are used to control applications and configure the application for a specific local use. This flow also supports remote control of the application so the application can be taken offline, reset, or restarted.
d) **RSE Application Install/Upgrade.** This flow supports remote installation and update of software applications residing in the RSE. It supports transmission of the secure software installation files, including executable application code and associated support files.
e) **RSE Application Status.** Monitoring of RSE application status including current mode, operational status, and configuration settings. It includes the status of installed applications and the application-specific data provided by the RSE.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

f) **RSE Configuration Settings.** Control settings and parameters that are used to configure roadside equipment.
g) **RSE Status.** Monitoring of RSE device status including current mode, operational status, and configuration settings. It includes device housekeeping/heartbeat monitoring and includes network information, the status of installed applications, the configuration of managed devices, cybersecurity and physical security status of the RSE.

The main user need groups (features), as identified in Section 2.5, are related to the information flows as shown in Table 1. There are more than 300 ARC-IT triples that include Connected Vehicle Roadside Equipment, which represents an RSU. Each information flow triple represents a source and destination Physical Object and the information flow that is exchanged. Of these, ten (10) triples are addressed by the NTCIP 1218 v01.

Table 1 Data Flows from ARC-IT

User Need Group	Source	Information Flow	Destination
Manage the RSU Configuration	CEN	RSE Application Information	CVRE
Manage the RSU Configuration	CEN	RSE Application Install/Upgrade	CVRE
Manage the RSU Configuration	FME	RSE Application Install/Upgrade	CVRE
Manage the RSU Configuration	FME	RSE Configuration Settings	CVRE
Monitor the RSU	CVRE	Device Identification	CEN
Monitor the RSU	CVRE	RSE Application Status	CEN
Monitor the RSU	CVRE	RSE Status	FME
Monitor the RSU	CVRE	RSE Status	SMS
Control the RSU	CEN	Equipment Control Commands	CVRE
Control the RSU	FME	Equipment Control Commands	CVRE

Where:

CEN = Center
CVRE = Connected Vehicle Roadside Equipment
FME = Field Maintenance Equipment
SMS = Service Monitor System

Figure 5 represents the physical view of the RSU system as depicted in ARC-IT. Figure 5is similar to Figure 1 with the addition of Support Services, which represents the security and directory services in this diagram.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

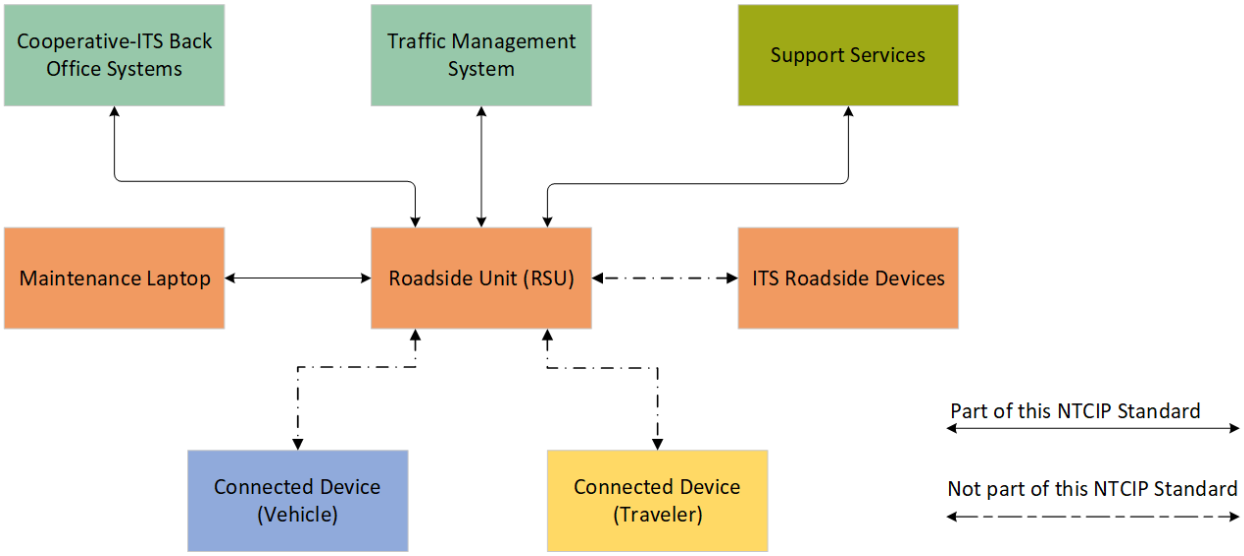

Figure 5 ARC-IT Physical View

© 2020 AASHTO / ITE / NEMA

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). Section 3 includes:

a) A tutorial
b) Protocol Requirements List (PRL) – 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 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 an RSU system or can be used by a manufacturer to document the features supported by their implementation.
c) Architectural Requirements – These are requirements related to the architectural needs defined in Section 2.4.
d) Data Exchange and Operational Environment Requirements – These are requirements related to the features identified in Sections 2.5 and 2.6 that can be realized through a data exchange. For example, this includes the requirement to be able to monitor what signal indications are active.
e) Supplemental Non-communications Requirements – These are additional requirements derived from the Concept of Operations that do not fall into one of the above two categories. For example, they include requirements related to performance requirements.

Section 3 is intended for all readers, including:

a) Transportation Managers
b) Transportation Operators
c) Transportation Engineers
d) Maintenance Personnel
e) System Integrators
f) Device Manufacturers

For the first four categories of readers, Section 3 is useful in understanding the details that NTCIP 1218 v01 requires of an RSU. For these readers, Section 3.3.3 is particularly useful in preparing procurement specifications and assists in mapping the various rows of this table to the more detailed text contained within the other sections.

For the last two categories of readers, this section is useful to fully understand what is required of equipment meeting this interface standard. Table 6 in Section 3.3.3 may be used to document the capabilities of their implementations.

3.1 Tutorial [Informative]

This Functional Requirements section defines the formal requirements that are intended to satisfy the user needs identified in Section 2. This is achieved through the development of a PRL that traces each user need to one or more requirements defined in this section. The details of each requirement are then presented following the PRL. The functional requirements are presented in three broad categories as follows:

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

a) Architectural Requirements – These requirements define the required behavior of the system in exchanging data across the communications interface, including any restrictions to general architectural requirements, based upon the architectural needs identified in the Concept of Operations.
b) Data Exchange Requirements – These requirements define the required behavior of the system in exchanging data across the communications interface based upon the features identified in the Concept of Operations.
c) Supplemental Requirements – These requirements define additional requirements of the system that are derived from the architectural and/or data exchange requirements but are not themselves architectural or data exchange requirements. A given supplemental requirement may relate to multiple architectural and/or data exchange requirements. Supplemental requirements include capabilities of the equipment (e.g., service processing or clearing expired priority requests) and security functions.

3.2 Scope of The Interface [Informative]

NTCIP 1218 v01 specifies the logical interface between an RSU and a controlling management station, such as a central management system. NTCIP 1218 v01 defines information that may be exchanged across this interface to allow a management station to configure, monitor, and control the RSU, as described by the features in Sections 2.5 and 2.6.

NTCIP 1218 v01 is only one component for defining the complete functions and capabilities of a deployed RSU. NTCIP 1218 v01 does not for example, address the communications interface between the RSU and the connected devices, such as an OBU; nor the communications interface between the RSU and other ITS Roadside Devices. Those communications interfaces are addressed by other standards, such as IEEE 802.11, IEEE 1609.x, SAE J2735, and SAE J2945 for the interface between the RSU and connected devices. However, NTCIP 1218 v01 does address the configuration of the RSU to enable communications across that interface.

NTCIP 1218 v01 also only addresses a small portion of the security system for an RSU and the overall connected vehicle environment. Security is a crucial consideration in the deployment of the connected vehicle environment. A security system in the connected vehicle environment allows the exchange of trusted data in a safe, secure manner without compromising privacy. NTCIP 1218 v01 only addresses security for the RSU as related to those functions that can be configured by a Management Information Base (MIB) and functions related to machine-to-machine connections (i.e., NTCIP 1218 v01 does not address human-to-machine connections).

NTCIP 1218 v01 does support uploading an application to an RSU and to determine if an application is running on the RSU. However, NTCIP 1218 v01 does not address the configuration of the application, or the specifications for application that may reside on an RSU (i.e., it does not address what applications should be on an RSU).

As a communications interface, NTCIP 1218 v01 also does not address hardware, mechanical or electrical requirements for an RSU, nor does it address the communications performance of the wireless radio.

3.3 Protocol Requirements List (PRL)

The PRL, provided in Table 6 defined in Section 3.3.3, maps the user needs defined in Section 2 to the requirements defined in Section 3. The PRL 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.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

c) The device manufacturer and user, as a detailed indication of the capabilities of the implementation.
d) The user, as a basis for initially checking the potential interoperability with another implementation.
e) The tester, as a checklist to compare against a specification and provide basis for test planning

3.3.1 Notation [Informative]

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 NTCIP 1218 v01.

3.3.1.1 Conformance Symbols

The symbols in Table 2 are used to indicate status under the Conformance column in the PRL.

Table 2 Conformance Symbols

Symbol	Status
M	Mandatory
M.#	Support of every item of the group labeled by the same numeral # is 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
NA	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 shall 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."

3.3.1.2 Conditional Status Notation

The predicate notations in Table 3 may be used.

Table 3 Conditional Status Notation

Predicate	Notation
<predicate>:	This notation introduces a single item that is conditional on the <predicate>.
<predicate>::	This notation introduces a table or a group of tables, all of which are conditional on the <predicate>.
(predicate)	This notation introduces the first occurrence of the predicate. The feature associated with this notation is the base feature for all options that have this predicate in their conformance column.

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 <predicate> notation may precede a table or group of tables in a section or subsection. When the group predicate is true then the associated section shall be completed.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

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 NTCIP 1218 v01 map to the sections indicated in Table 4.

Table 4 Predicate Mapping to NTCIP 1218 v01 Section

Predicate	Section
Alternating	3.5.1.3.3.3.2 (If Alternating is selected)
DSRC	2.3.2.a
GNSSOut	3.5.1.1.3.6.1
Inform	3.5.1.1.7.4
LongLoss	3.5.1.1.6.2
PC5	2.3.2.b
ShortLoss	3.5.1.1.6.1
StartupFault	3.5.1.1.4.4
Temp	3.5.2.10.1

3.3.1.3 Support Column Symbols

The Support column in the PRL 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:

Table 5 Support Column Entries

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

3.3.2 Instructions for Completing the PRL [Informative]

In the ‘Support’ 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 (for example, list of traffic signal controllers to be supported by an implementation).

If a conditional requirement is inapplicable, use the Not Applicable (NA) choice. If a mandatory requirement is not satisfied, exception information shall 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 (as defined in 3.3.1.1 above), the response shall address each element of the requirement; e.g., for the requirement "mo," the possible compliant responses are "yy" or "yn."

> Note: A specification can allow for flexibility in a deliverable by leaving the selection in the Support column blank for a given row.

3.3.2.1 Conformance Definition

To claim "Conformance" to NTCIP 1218 v01, the manufacturer shall minimally fulfill the mandatory requirements as identified in the PRL table (see Table 6).

> Note: The reader and user of NTCIP 1218 v01 is advised that 'conformance' to NTCIP 1218 v01 should not be confused with 'compliance' to a specification. NTCIP 1218 v01 is as broad as

 © 2020 AASHTO / ITE / NEMA

possible to allow a very simple RSU implementation to be 'conformant' to NTCIP 1218 v01. An agency specification needs to identify the requirements of a particular project and needs to require the support of those requirements. A specification writer is advised to match the requirements of a project with the corresponding standardized requirements defined in NTCIP 1218 v01 to achieve interoperability. This means that functions and requirements defined as 'optional' in NTCIP 1218 v01 might need to be selected in a specification (in effect made 'mandatory' for the project-specific specification).

A conformant device may offer additional (optional) features, as long as they are conformant with the requirements of NTCIP 1218 v01 and the standards it references (e.g., NTCIP 1201 v03). For example, to claim conformance to additional features, an implementation shall conform to all of the mandatory and selected optional requirements that trace to the subject user needs in the PRL, AND shall fulfill the requirement by using all of the dialogs and data elements traced to the subject requirement in the Requirements Traceability Matrix (RTM) in Annex A.

A device may also support data that has not been defined by NTCIP 1218 v01; however, when exchanged via an SNMP-like protocol, the data shall 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 through well documented features broadly supported by the industry as a whole. Designing a system that uses features not defined in a standard or not typically deployed in combination with one another inhibits the goals of interoperability and interchangeability, especially if the documentation of these features is not available for distribution to system integrators. Standards allow the use of additional features to support innovation, which is constantly needed within the industry; but users should be aware of the risks involved with using such features.

To claim "Conformance" to NTCIP 1218 v01, an RSU device shall be provided with a MIB that contains all non-NTCIP-standardized (including custom, proprietary and manufacturer-, agency-, or implementation-specific) object and block definitions. Object and block definitions contained in the MIB shall:

a) use the ASN.1 notation and conventions used in NTCIP 1218 v01 standardized object and block definitions,
b) include non-NTCIP-standardized enumerations, and
c) include meaningful, human-understandable, English language DESCRIPTION fields including descriptions of the object and all supported values.

In addition, to claim "Conformance" to NTCIP 1218 v01, an RSU device shall use the NTCIP 1218 v01 standardized objects to manage NTCIP 1218 v01 functionality. Non-NTCIP-standardized objects may be used to manage NTCIP 1218 v01 functionality only if NTCIP 1218 v01 standardized objects for the same functions are also supported. RSU devices or systems attempting to manage, configure, or monitor an NTCIP 1218 v01 standardized object shall not be required to use proprietary objects for NTCIP 1218 v01 functionality.

3.3.3 Protocol Requirements List (PRL) Table

In addition to the Conformance column and the Support column, which were discussed in Sections 3.3.1 and 3.3.2, the additional columns in the PRL table are the User Need ID and User Need columns, FR ID and Functional Requirements columns and the Additional Specifications column.

a) User Need ID - the number assigned to the user need statement. The user needs are defined within Section 2 and the PRL is based upon the user need sections within that Section.
b) User Need – a short descriptive title identifying the user need.
c) FR ID – the number assigned to the functional requirement statement. The requirements are defined within Section 3 and the PRL references the traces from user needs to these requirements.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

d) Functional Requirement – a short descriptive title identifying the functional requirement.
e) Additional Specifications - identifies other requirements to satisfy, including user selectable range values. The "Additional Specifications" column may (and should) be used by a procurement specification to provide additional notes and requirements for the product to be procured or may be used by an implementer to provide any additional details about the implementation. In some cases, default text already exists in this field, which the user should complete to fully specify the equipment. However, additional text can be added to this field as needed to fully specify a feature.

Note: Visit www.ntcip.org for information on availability of electronic copies of the PRL.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

Table 6 Protocol Requirements List (PRL)

Protocol Requirements List (PRL)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
2.3	Reference Physical Architecture [Informative]					
2.3.1	RSU Characteristics - General					
2.3.2	RSU Characteristics - V2X Radio Type			M	Yes	
2.3.2.a (DSRC)	DSRC Radio			O.1 (1)	Yes / No	Also see 3.5.1.3.1.2.
2.3.2.b (PC5)	PC5 Radio			O.1 (1)	Yes / No	Also see 3.5.1.3.1.2.
2.4	Architectural Needs					
2.4.1	Configure, Monitor and Control the RSU			M	Yes	
		3.4.1.1	Retrieve Data	M	Yes	
		3.4.1.2	Deliver Data	M	Yes	
		3.4.1.3	Explore Data	M	Yes	
		3.6.2	Response Time for Requests	M	Yes	The Response Time for all requests shall be ___ milliseconds (5-2000: Default=1000).
2.4.2	Provide for Log Data Local Storage and Retrieval			M	Yes	
		3.4.2.1	Configure Priority Level for Events	M	Yes	
		3.4.2.2	Close an Active Event Log File	C	Yes / No / NA	If the event log implementation supports the capability to close an active system log file.
		3.4.2.3	Retrieve Event Logged Data	M	Yes	
		3.6.3.1	Event Log - System Events	M	Yes	
		3.6.3.2	Event Log - Application Events	M	Yes	
		3.6.3.3	Event Log - RSU Configuration	M	Yes	
		3.6.3.4	Event Log - Notification	M	Yes	
		3.6.3.5	Event Log - Security	M	Yes	
		3.6.3.6	Event Log - Stored Message	M	Yes	
		3.6.3.7	Event Log - Immediate Forward Message	M	Yes	

© 2020 AASHTO / ITE / NEMA Copy Per PRL Distribution Permission

Protocol Requirements List (PRL)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		3.6.2	Response Time for Requests	M	Yes	The Response Time for all requests shall be ___ milliseconds (5-2000: Default=1000).
2.4.3	Condition-based Exception Reporting			M	Yes	
		3.4.3	Condition-based Exception Reporting	M	Yes	
2.5	Features					
2.5.1	Manage the RSU Configuration			M	Yes	
2.5.1.1	Manage the RSU Device			M	Yes	
2.5.1.1.1	Retrieve RSU Identity			M	Yes	
		3.5.1.1.1.1	Store RSU Identifier	M	Yes	
		3.5.1.1.1.2	Report RSU Component Information	M	Yes	
		3.5.1.1.1.3	Report Supported Standards	O	Yes / No	
		3.5.1.1.1.4	Report RSU System Name	M	Yes	
		3.5.1.1.1.5	Report RSU MIB Version	O	Yes / No	
2.5.1.1.2	Retrieve Configuration Version of the RSU			M	Yes	
		3.5.1.1.2	Report Deployment Configuration Identifier	M	Yes	
2.5.1.1.3	Manage RSU Location Information			M	Yes	
		3.5.1.1.3.1	Store RSU Location Description	O	Yes / No	
		3.5.1.1.3.2	Store RSU Location	M	Yes	
		3.5.1.1.3.3	Store RSU Location - GNSS Antenna Offset	O	Yes / No	
		3.5.1.1.3.4	Store V2X Antenna Offsets	O	Yes / No	
		3.5.1.1.3.5	Report Positioning Augmentation	O	Yes / No	
		3.5.1.1.3.6.1 (GNSSOut)	Store GNSS Data Output Destination	O	Yes / No	The format of the GNSS data shall be: _____ (Default: GPGGA NMEA String)
		3.5.1.1.3.6.2	Report GNSS Data Output	GNSSOut:O	Yes / No / NA	
		3.5.1.1.3.6.3	Store GNSS Data Output Interval	GNSSOut:O	Yes / No / NA	
		3.5.2.4.1	Report RSU Location	M	Yes	
2.5.1.1.4	Manage RSU Startup Functions			O	Yes / No	
		3.5.1.1.4.1	Determine Maximum Number of Applications Supported	M	Yes	The RSU shall support a minimum of _____ (Default: 5) applications.

Copy Per PRL Distribution Permission
© 2020 AASHTO / ITE / NEMA

Protocol Requirements List (PRL)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		3.5.1.1.4.2	Manage RSU Startup Functions - Applications	M	Yes	Applications that shall be configured to automatically start: _____ _____ _____
		3.5.1.1.4.3	Manage RSU Startup Functions - Configuration File	O	Yes / No	
		3.5.1.1.4.4 (StartupFault)	Configure Startup Retries	O	Yes / No	
		3.5.1.1.4.5	Retrieve Startup Retry Period	StartupFault:M	Yes / NA	
		3.6.5	Copy Files using SCP	M	Yes	
2.5.1.1.5	Manage RSU Firmware Version			M	Yes	
		3.5.1.1.5.1	Report the RSU Firmware Version	M	Yes	
		3.5.1.1.5.2	Update the RSU Firmware Version	M	Yes	
		3.5.1.1.5.3	Report Firmware Update Status	M	Yes	
		3.6.5	Copy Files using SCP	M	Yes	
2.5.1.1.6	Manage Communications Loss			O	Yes / No	
		3.5.1.1.6.1 (ShortLoss)	Configure Short-Term Communications Loss	O.2 (1..*)	Yes / No	
		3.5.1.1.6.2 (LongLoss)	Configure Long-Term Communications Loss	O.2 (1..*)	Yes / No	
		3.5.1.1.6.3	Configure Short-Term Communications Event for Stored Messages	ShortLoss:M	Yes / NA	
		3.5.1.1.6.4	Configure Long-Term Communications Event for Stored Messages	LongLoss:M	Yes / NA	
		3.5.1.1.6.5	Configure Short-Term Communications Event for Immediate Forward Messages	ShortLoss:M	Yes / NA	
		3.5.1.1.6.6	Configure Long-Term Communications Event for Immediate Forward Messages	LongLoss:M	Yes / NA	
		3.5.1.1.6.7	Configure Long-Term Communications Event for Reboot	LongLoss:O	Yes / No / NA	
2.5.1.1.7	Manage Notifications			M	Yes	

© 2020 AASHTO / ITE / NEMA

Protocol Requirements List (PRL)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		3.5.1.1.7.1	Store Notification Destination Address	M	Yes	
		3.5.1.1.7.2	Store Notification Destination Port	M	Yes	
		3.5.1.1.7.3.1	Notification - Integrity Check Error - Active Message	M	Yes	
		3.5.1.1.7.3.2	Notification - Integrity Check Error - Secure Storage	M	Yes	
		3.5.1.1.7.3.3	Notification - Authorization Verification Error	M	Yes	
		3.5.1.1.7.3.4	Notification - Signature Verification Error	M	Yes	
		3.5.1.1.7.3.5	Notification - Network Access Control List	M	Yes	
		3.5.1.1.7.3.6	Notification - Time Source Loss	M	Yes	
		3.5.1.1.7.3.7	Notification - Time Source Mismatch	M	Yes	
		3.5.1.1.7.3.8	Notification - GNSS Anomaly	M	Yes	
		3.5.1.1.7.3.9	Notification - GNSS Location Deviation	M	Yes	
		3.5.1.1.7.3.10	Notification - Certificate Management	M	Yes	
		3.5.1.1.7.3.11	Notification - Denial of Service	O	Yes / No	
		3.5.1.1.7.3.12	Notification - Watchdog	O	Yes / No	
		3.5.1.1.7.3.13	Notification - GNSS Data	O	Yes / No	
		3.5.1.1.7.3.14	Notification - Configure GNSS Data Interval	O	Yes / No	
		3.5.1.1.7.3.15	Notification - Environmental	O	Yes / No	
		3.5.1.1.7.3.16	Notification - Authentication Failure	M	Yes	
		3.5.1.1.7.4 (Inform)	Store Notification Type	O	Yes / No	
		3.5.1.1.7.5	Store Notification Repeat Intervals	Inform:M	Yes / No / NA	
		3.5.1.1.7.6	Store Notification Retries	Inform:M	Yes / No / NA	
2.5.1.2	Manage Network Interface					
2.5.1.2.1	Manage a Network Interface			M	Yes	
		3.5.1.2.1.1	Enable/Disable a Communications Port	M	Yes	
		3.5.1.2.1.2	Configure Ethernet Ports	M	Yes	

© 2020 AASHTO / ITE / NEMA

Protocol Requirements List (PRL)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		3.5.1.2.1.3	Report Ethernet Port - MAC Address	M	Yes	
2.5.1.2.2	Manage Messages					
2.5.1.2.2.1	Manage Stored Messages			M	Yes	
		3.5.1.2.2.1.1	Determine Maximum Number of Stored Messages Supported	M	Yes	The RSU shall have support a minimum of _____ (Default: 100) stored messages.
		3.5.1.2.2.1.2	Store a Message	M	Yes	
		3.5.1.2.2.1.3	Delete a Stored Message	M	Yes	
		3.5.1.2.2.1.4	Enable/Disable the Transmission of a Stored Message	M	Yes	
		3.5.1.2.2.1.5	Store a Message Type	M	Yes	
		3.5.1.2.2.1.6	Store PSID for Application Data Exchanges	M	Yes	
		3.5.1.2.2.1.7	Delete All Stored Messages	O	Yes / No	
2.5.1.2.2.2	Manage Stored Messages for Transmission			M	Yes	
		3.5.1.2.2.1.6	Store PSID for Application Data Exchanges	M	Yes	
		3.5.1.2.2.1.7	Delete All Stored Messages	O	Yes / No	
		3.5.1.2.2.1.8	Store a Message's Priority	M	Yes	
		3.5.1.2.2.1.9	Store a Message's Transmission Interval	M	Yes	
		3.5.1.2.2.1.10	Store a Message's Transmission Channel	M	Yes	
		3.5.1.2.2.1.11	Store a Message's Transmission Start Time	M	Yes	
		3.5.1.2.2.1.12	Store a Message's Transmission Stop Time	M	Yes	
		3.5.1.2.2.1.13	Store if a Message is to be Signed	M	Yes	
2.5.1.2.2.3	Manage Received Messages for Forwarding to the V2X Interface			M	Yes	
		3.5.1.2.2.2.1	Determine Maximum Number of Immediate Forward Messages Supported	M	Yes	The RSU shall have support a minimum of _____ (Default: 100) messages for forwarding.
		3.5.1.2.2.2.2	Forward Message to the V2X Interface	M	Yes	

© 2020 AASHTO / ITE / NEMA

Protocol Requirements List (PRL)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		3.5.1.2.2.2.3	Store the Message Type for a Message for Forwarding to the V2X Interface	M	Yes	
		3.5.1.2.2.2.4	Store the PSID for an Application Data Exchange for Forwarding to the V2X Interface	M	Yes	
		3.5.1.2.2.2.5	Store the Priority for a Message for Forwarding to the V2X Interface	O	Yes / No	
		3.5.1.2.2.2.6	Store the Transmission Channel for a Message for Forwarding to the V2X Interface	M	Yes	
		3.5.1.2.2.2.7	Store if a Received Message for Forwarding to the V2X Interface is Signed	M	Yes	
2.5.1.2.2.4	Manage Received Messages from the V2X Interface for Forwarding			M	Yes	
		3.5.1.2.2.3.1	Determine Maximum Number of Message Received Types Supported	M	Yes	
		3.5.1.2.2.3.2	Store Network Destination to Forward Messages Received from the V2X Interface	M	Yes	
		3.5.1.2.2.3.3	Store Transport Protocol to Forward Messages Received from the V2X Interface	O	Yes / No	
		3.5.1.2.2.3.4	Store Minimum Signal Strength to Forward Messages Received from the V2X Interface	O	Yes / No	
		3.5.1.2.2.3.5	Store Message Interval to Forward Messages Received from the V2X Interface	O	Yes / No	
		3.5.1.2.2.3.6	Store Start Time to Forward Messages Received from the V2X Interface	M	Yes	
		3.5.1.2.2.3.7	Store Stop Time to Forward Messages Received from the V2X Interface	M	Yes	

Copy Per PRL Distribution Permission
© 2020 AASHTO / ITE / NEMA

Protocol Requirements List (PRL)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		3.5.1.2.2.3.8	Enable/Disable Forwarding Messages Received from the V2X Interface	M	Yes	
		3.5.1.2.2.3.9	Store Secure Options to Forward Messages Received from the V2X Interface	O	Yes / No	
		3.5.1.2.2.3.10	Store Interval to Authenticate Messages Received from the V2X Interface	O	Yes / No	
2.5.1.2.2.5	Manage Transmitted Messages over the V2X Interface for Forwarding			O	Yes / No	
		3.5.1.2.2.4.1	Determine Maximum Number of Message Entries Transmitted Over the V2X Interface For Forwarding Supported	M	Yes	
		3.5.1.2.2.4.2	Store Network Destination to Forward Messages Transmitted Over the V2X Interface	M	Yes	
		3.5.1.2.2.4.3	Store Transport Protocol to Forward Messages Transmitted Over the V2X Interface	M	Yes	
		3.5.1.2.2.4.4	Store Start Time to Forward Messages Transmitted Over the V2X Interface	M	Yes	
		3.5.1.2.2.4.5	Store Stop Time to Forward Messages Transmitted Over the V2X Interface	M	Yes	
2.5.1.2.3	Manage Logging of Interface Data			O	Yes / No	
		3.5.1.2.3.1	Determine Maximum Number of Interface Logs Supported	M	Yes	The RSU shall have support a minimum of _____ (1-255: Default=4) simultaneous recordings.
		3.5.1.2.3.2	Log Interface Data Identification	M	Yes	
		3.5.1.2.3.3	Log Interface Data by Direction	O	Yes / No	
		3.5.1.2.3.4	Store Interface Data Log - File Directory	O	Yes / No	

© 2020 AASHTO / ITE / NEMA

Protocol Requirements List (PRL)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		3.5.1.2.3.5	Retrieve Interface Logged Data	M	Yes	
		3.5.1.2.3.6	Store an Interface Data Log Start Time	O	Yes / No	
		3.5.1.2.3.7	Store an Interface Data Log Stop Time	O	Yes / No	
		3.5.1.2.3.8	Store Maximum Interface Data Log File Size	O	Yes / No	The RSU shall support a maximum interface data log file size of: (1-40: Default=20) _____ MB.
		3.5.1.2.3.9	Store Maximum Interface Data Log File Collection Time	O	Yes / No	The RSU shall support a maximum interface data log collection time of: (1-48: Default=12) _____ hours.
		3.5.1.2.3.10	Store Interface Data Log Option - Disk Full	O	Yes / No	
		3.5.1.2.3.11	Store Interface Data Log Option - Entry Deletion	O	Yes / No	
		3.6.4.1	Interface Data Log Format	M	Yes	
		3.6.4.2	Interface Data Log File Format	M	Yes	
		3.6.4.3.1	Support RSU Identifier in the Interface Data Log Filename	M	Yes	
		3.6.4.3.2	Support Interface Identifier in the Interface Data Log Filename	M	Yes	
		3.6.4.3.3	Support Direction in the Interface Data Log Filename	M	Yes	
		3.6.4.3.4	Support Date and Time in the Interface Data Log Filename	M	Yes	
		3.6.4.4	Interface Data Logging - Operational State	O	Yes / No	
		3.6.4.5	Open a New Interface Data Log	M	Yes	
		3.6.5	Copy Files using SCP	M	Yes	
2.5.1.3	Configure V2X Interface					
2.5.1.3.1	Enable/Disable Radios			M	Yes	

© 2020 AASHTO / ITE / NEMA

Protocol Requirements List (PRL)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		3.5.1.3.1.1	Report Maximum Number of V2X Radios Supported	M	Yes	The RSU shall support _____ (1-16) V2X radios.
		3.5.1.3.1.2	Report Type of V2X Radio	M	Yes	Also see 2.3.2.
		3.5.1.3.1.3	Enable/Disable Radios	M	Yes	
		3.5.1.3.1.4	Report Radio MAC Address	DSRC:M	Yes / NA	
		3.5.1.3.1.5	Report Radio Operating Modes	O	Yes / No	
2.5.1.3.2	Determine Lower Layer Parameters			O	Yes / No	
		3.5.1.3.2.1	Determine Lower Layer Parameter	DSRC:M	Yes / NA	
		3.5.1.3.2.2	Determine Operating Class	O	Yes / No	
2.5.1.3.3	Configure IEEE 1609 Communications					
2.5.1.3.3.1	Configure IEEE 1609.2 Security			M	Yes	
		3.5.1.3.3.1.1	Report IEEE 1609.2 Enrollment Certificate - Status	M	Yes	
		3.5.1.3.3.1.2	Report IEEE 1609.2 Enrollment Certificate - Expiration Date	M	Yes	
		3.5.1.3.3.1.3	Report IEEE 1609.2 Enrollment Certificate - Source Domain	M	Yes	
		3.5.1.3.3.1.4	Report IEEE 1609.2 Enrollment Certificate Identifier	M	Yes	
		3.5.1.3.3.1.5	Report IEEE 1609.2 Enrollment Certificate - Valid Region	M	Yes	
		3.5.1.3.3.1.6	Report IEEE 1609.2 Enrollment Certificate - Source	M	Yes	
		3.5.1.3.3.1.7	Report IEEE 1609.2 Application Certificates - Status	M	Yes	
		3.5.1.3.3.1.8	Report IEEE 1609.2 Application Certificates - Source	M	Yes	
		3.5.1.3.3.1.9	Store IEEE 1609.2 Application Certificates - Default Request Interval	M	Yes	
		3.5.1.3.3.1.10	Store IEEE 1609.2 Application Certificates - Request Interval	O	Yes / No	
		3.5.1.3.3.1.11	Report Certificate Revocation List - Source	M	Yes	
		3.5.1.3.3.1.12	Report Certificate Revocation List - Update Time	M	Yes	

© 2020 AASHTO / ITE / NEMA

Protocol Requirements List (PRL)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		3.5.1.3.3.1.13	Store Certificate Revocation List Update Interval	M	Yes	
		3.5.1.3.3.1.14	Update Certificate Revocation List Command	M	Yes	
		3.5.1.3.3.1.15	Report IEEE 1609.2 Security Profiles	M	Yes	
		3.6.8	Determine Maximum Number of Application Certificates Supported	M	Yes	The RSU shall be able to store at least ___ application certificates.
2.5.1.3.3.2	Configure IEEE 1609.3 Communications - WSA			M	Yes	
		3.5.1.3.3.2.1	Determine Maximum Number of Services Advertised	M	Yes	
		3.5.1.3.3.2.2	Store WSA Configuration - Service Info Segment	O	Yes / No	
		3.5.1.3.3.2.3	Store WSA Configuration - Channel Info Segment	O	Yes / No	
		3.5.1.3.3.2.4	Configure WSA Configuration - WAVE Router Advertisement	O	Yes / No	
		3.5.1.3.3.2.5	Store WSA Configuration - Secure	M	Yes	
		3.5.1.3.3.2.6	Report WSA Version Number	M	Yes	
2.5.1.3.3.3	Configure IEEE 1609.4 Communications			DSRC:M	Yes / NA	
		3.5.1.3.3.3.1	Store the IEEE 1609.4 Configuration for a Radio	M	Yes	
		3.5.1.3.3.3.2	Store Radio Channel Access Mode	M	Yes	Each radio supports the following modes: __ Continuous OR __ Alternating (Alternating) The following are optional. ____ Immediate ____ ImmediateAndExtended
		3.6.7	Time Fix - Alternating Mode	Alternating:M	Yes / NA	
2.5.1.3.3.4	Configure Radio Transmitter Properties			O	Yes / No	
		3.5.1.3.4.1	Store Default Transmit Power	M	Yes	
		3.5.1.3.4.2	Report Maximum Number of V2X Antennas Supported	O	Yes / No	

© 2020 AASHTO / ITE / NEMA

Protocol Requirements List (PRL)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		3.5.1.3.4.3	Store Antenna Gain and Cable Losses	O	Yes / No	
		3.5.1.3.4.4	Store Antenna Type	O	Yes / No	
2.5.1.4	Manage RSU Applications			O	Yes / No	
2.5.1.4.1	Manage RSU Application			M	Yes	
		3.5.1.4.1.1	Install an RSU Application	M	Yes	
		3.5.1.4.1.2	Report Software Update Status	M	Yes	
		3.6.5	Copy Files using SCP	M	Yes	
2.5.1.4.2	Save and Restore Application Configuration			M	Yes	
		3.5.1.4.2.1	Install a Configuration File	M	Yes	
		3.5.1.4.2.2	Report Configuration File Update Status	M	Yes	
		3.6.5	Copy Files using SCP	M	Yes	
2.5.1.5	Manage Location Corrections			O	Yes / No	
		3.5.1.5.1	Forward Location Corrections Data	M	Yes	
		3.5.1.5.2	Use RTCM Corrections Data	M	Yes	Location corrections data type: _____ (e.g., RTCMcorrections as defined in SAE J2735_2016).
2.5.2	Monitor the RSU					
2.5.2.1	Determine RSU Operational Performance Status			O	Yes / No	
		3.5.2.1.1	Report Time Elapsed Since RSU Power On	M	Yes	
		3.5.2.1.2	Report Amount of Free Memory	O	Yes / No	
		3.5.2.1.3	Report Instantaneous CPU Load	O	Yes / No	
		3.5.2.1.4	Report CPU Load Average - 15 Minutes	O	Yes / No	
		3.5.2.1.5	Report CPU Load Average - 5 Minutes	O	Yes / No	
		3.5.2.1.6	Report CPU Load Average - 1 Minute	O	Yes / No	
		3.5.2.1.7	Report Storage Space Available	O	Yes / No	
		3.5.2.1.8	Report Number of Messages Exchanged	O	Yes / No	
2.5.2.2	Determine Mode of Operations			M	Yes	
		3.5.2.2	Report Mode of Operations	M	Yes	

© 2020 AASHTO / ITE / NEMA

Protocol Requirements List (PRL)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
2.5.2.3	Determine RSU Clock Status			O	Yes / No	
		3.5.2.3.1	Report RSU Clock Source	M	Yes	Time source: _____. Default: UTC with epoch 1, January 1970 00:00:00.
		3.5.2.3.2	Report RSU Clock Status	M	Yes	
		3.5.2.3.3	Store Allowable RSU Clock Source Timeout	O	Yes / No	
		3.5.2.3.4	Store Allowable RSU Clock Source Queries	O	Yes / No	
		3.5.2.3.5	Store Allowable Time Deviation	O	Yes / No	
2.5.2.4	Determine RSU Location			M	Yes	
		3.5.2.4.1	Report RSU Location	M	Yes	Minimum sample rate for GNSS or similar geopositioning device: _____ (Default: 1 Hz)
		3.5.2.4.2	Report Positioning Status	M	Yes	
		3.5.2.4.3	Store Allowable RSU Location Tolerance	O	Yes / No	
		3.5.2.4.4	Report RSU Location Deviation	O	Yes / No	
		3.5.2.4.5	Report RSU Estimated Location Error	O	Yes / No	
2.5.2.5	Monitor Network Interfaces			O	Yes / No	
		3.5.2.5.1	Monitor Data Link Errors - Ethernet	M	Yes	
2.5.2.6	Report Number of Messages Exchanged			O	Yes / No	
		3.5.2.1.8	Report Number of Messages Exchanged	O	Yes / No	
		3.5.2.6	Report Number of Messages Exchanged by V2X Radio and PSID	M	Yes	
2.5.2.7	Determine Number of Active Radios			O	Yes / No	
		3.5.2.7	Determine Number of Active Radios	M	Yes	
2.5.2.8	Determine RF Communications Range			O	Yes / No	
		3.5.2.8.1	Determine Maximum Number of Communications Range Entries	M	Yes	
		3.5.2.8.2	Report the RF Communications Distance - 1 Minute	O	Yes / No	
		3.5.2.8.3	Report the RF Communications Distance - 5 Minutes	O	Yes / No	

Copy Per PRL Distribution Permission
© 2020 AASHTO / ITE / NEMA

Protocol Requirements List (PRL)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		3.5.2.8.4	Report the RF Communications Distance - 15 Minutes	O	Yes / No	
		3.5.2.8.5	Report the Average RF Communications Distance - 1 Minute	O	Yes / No	
		3.5.2.8.6	Report the Average RF Communications Distance - 5 Minutes	O	Yes / No	
		3.5.2.8.7	Report the Average RF Communications Distance - 15 Minutes	M	Yes	
2.5.2.9	Determine Application Status			M	Yes	
		3.5.2.9	Determine Application Status	M	Yes	
2.5.2.10	Determine RSU Environment			O	Yes / No	
		3.5.2.10.1 (Temp)	Report the Internal Operating Temperature	C	Yes / No / NA	If equipped.
		3.5.2.10.2	Determine the Internal Operating Temperature Thresholds	Temp:O	Yes / No / NA	
		3.5.1.1.7.3.15	Notification - Environmental	Temp:O	Yes / No / NA	
2.5.2.11	Determine RSU Current Status			M	Yes	
		3.5.2.11	Report RSU Current Status Requirements	M	Yes	
2.5.3	Control the RSU					
2.5.3.1	Control Mode of Operation			M	Yes	
		3.5.3.1	Control Mode of Operation	M	Yes	
2.5.3.2	Control RF Antenna Output			O	Yes / No	
		3.5.3.2	Control RF Antenna Output	M	Yes	
2.5.3.3	Reboot RSU			M	Yes	
		3.5.3.3	Reboot RSU	M	Yes	
2.5.3.4	Control Application			O	Yes / No	
		3.5.3.4	Control Application	M	Yes	
2.6	Security					
2.6.1	Manage Authentication			M	Yes	
		3.5.1.1.7.3.4	Notification - Signature Verification Error	M	Yes	

© 2020 AASHTO / ITE / NEMA

Protocol Requirements List (PRL)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		3.5.1.1.7.3.10	Notification - Certificate Management	M	Yes	
		3.5.4.1.1.1	Valid Geographic Region - Enrollment Certificates	O	Yes / No	
		3.6.1.1.1	Support SHA-1	M	Yes	
		3.6.1.1.2	Support SHA-2	O	Yes / No	The RSU shall use (select one): ____ SHA-256 ____ SHA-384 ____ SHA-512 ____ SHA-512/224 ____ SHA-512/256
		3.6.6	User Accounts	M	Yes	The RSU shall support at least _____ (2..255) user accounts.
2.6.2	Manage Data Integrity			M	Yes	
		3.5.1.1.7.3.1	Notification - Integrity Check Error - Active Message	M	Yes	
		3.5.1.1.7.3.2	Notification - Integrity Check Error - Secure Storage	M	Yes	
		3.6.1.2.1	Access RSU - USM	M	Yes	
2.6.3	Manage Availability			M	Yes	
		3.5.1.1.7.3.5	Notification - Network Access Control List	M	Yes	
		3.5.4.2.1	Report Expiration Date - Enrollment Certificates	M	Yes	
		3.5.4.2.2	Report Expiration Date - Application Certificates	M	Yes	
2.6.4	Manage Confidentiality			M	Yes	
		3.6.1.2.1	Access RSU - USM	M	Yes	
		3.6.1.2.2	Access RSU - TSM	M	Yes	
		3.6.1.2.3	Support AES-256 Encryption	M	Yes	
		3.6.1.2.4	Support DTLS	M	Yes	

Copy Per PRL Distribution Permission
© 2020 AASHTO / ITE / NEMA

3.4 Architectural Requirements

Requirements for communication capabilities follow.

3.4.1 Support Basic Communications Requirements

Requirements for a transportation manager and transportation operator to make requests to an RSU follow.

3.4.1.1 Retrieve Data

Upon request from a management station, the RSU shall provide the data requested. This is a high-level requirement. The exact detailed requirements for the RSU to provide the specific values of data requested are defined by numerous functional requirements found in Section 3.5, Data Exchange and Operational Environment Requirements.

3.4.1.2 Deliver Data

Upon request from a management station, the RSU shall receive the data (e.g., configuration data, commands, etc.) provided. This is a high-level requirement. The exact detailed requirements to store the specific values of data requested are defined by numerous functional requirements found in Section 3.5, Data Exchange and Operational Environment Requirements.

3.4.1.3 Explore Data

Upon request from a management station, the RSU shall allow dynamic discovery of the data concepts and data instances supported by the RSU. This requirement allows a management station to "walk" a MIB. This is a high-level requirement. The exact detailed requirements to report the data and data values supported are defined by numerous functional requirements found in Section 3.5, Data Exchange and Operational Environment Requirements.

3.4.2 Log Data Local Storage and Retrieval Requirements

Requirements for a transportation manager and transportation operator to configure and retrieve logged data from the RSU follow. The logged data contain information about the RSU and events that occur on the RSU.

3.4.2.1 Configure Priority Level for Events

Upon request from a management station, the RSU shall store the priority level of events that can be recorded for the event logging service. The valid priority levels are defined in RFC 5424. This requirement allows a manager to define the priority level of events recorded by the RSU.

3.4.2.2 Close an Active Event Log File

Upon request from a management station, the RSU shall command the open (active) event log file that the RSU is currently storing logged events to close, at the earliest convenient time.

> Note: Some event log implementations automatically close open event log files, and thus may not support this requirement.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

3.4.2.3 Retrieve Event Logged Data

Upon request from a management station, the RSU shall return the logged data from its event log. This requirement allows the management station to filter the logged data based on start and end times and by priority level.

3.4.3 Condition-based Exception Reporting

Upon detection of specified events, the RSU shall transmit a notification to a specified management station of the event occurrence. This is a high-level requirement. The exact detailed requirements to report the data and data values supported are defined by numerous functional requirements found in Section 3.5.1.1.7, Manage Notification Requirements.

3.5 Data Exchange and Operational Environment Requirements

Data exchange requirements for the RSU follow.

3.5.1 RSU Configuration Management Requirements

The requirements for managing the RSU configuration follow.

3.5.1.1 RSU Device Management Requirements

The requirements for managing the RSU device follow.

3.5.1.1.1 Retrieve RSU Identity Requirements

The requirements to identify the RSU follows.

3.5.1.1.1.1 Store RSU Identifier

Upon request from a management station, the RSU shall store its assigned identifier. The identifier is a text string from 0 to 32 characters in length.

3.5.1.1.1.2 Report RSU Component Information

Upon request from a management station, the RSU shall report the identification information for each module contained in the RSU. The identification information consists of:

a) The manufacturer of the module
b) The model number or firmware reference of the module
c) The version of the module
d) An indication of whether it is a software or hardware module

3.5.1.1.1.3 Report Supported Standards

Upon request from a management station, the RSU shall report the communications standards (and versions) supported by the RSU, with each communication standard indicator separated by a comma. The description consists of a text field up to 255 characters in length.

3.5.1.1.1.4 Report RSU System Name

Upon request from a management station, the RSU shall report the unique system name of the RSU. This system name could be any unique value such as a serial number up to 255 characters in length.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

3.5.1.1.1.5 Report RSU MIB Version

Upon request from a management station, the RSU shall report the identity and version of the MIB(s) in use. The module identity allows the manager to identify what version of a standard, as well as the standards and specifications it references; and what version of private objects are supported and referenced. The module identity is assigned by the manufacturer.

3.5.1.1.2 Report Deployment Configuration Identifier

Upon request from a management station, the RSU shall report the unique identifier created using a checksum-creation-like algorithm across all configuration parameters contained in the RSU database. The RSU creates the identifier at powerup and is updated whenever changes are made to any of the RSU configuration parameters.

The management station may use this unique identifier to determine if the current configuration of the RSU is as expected. If the reported unique identifier is different, then the configuration of the RSU may have changed, possibly as a result of a change initiated by another management station, such as a maintenance worker in the field.

> Note: For NTCIP 1218 v01, how the unique identifier is generated is allowed to be vendor-specific. This allows the vendor to include other parameters, which may be stored in vendor-specific (private) object identifiers or not stored in an object identifier, as part of the algorithm to generate the unique identifier. Any changes to a configuration (static) parameter should result in a change in the unique identifier.

3.5.1.1.3 Manage RSU Location Requirements

The requirements for managing the physical location of the RSU follow.

3.5.1.1.3.1 Store RSU Location Description

Upon request from a management station, the RSU shall store a textual description of its location. The description consists of a text field up to 140 characters in length.

3.5.1.1.3.2 Store RSU Location

Upon request from a management station, the RSU shall store its reference location, as provided within the request. The RSU location consists of the latitude, longitude, and elevation. The latitude and longitude are in tenths of a microdegree (10^-7 degrees) using the WGS-84 (World Geodetic System 1984). The elevation of the RSU is in centimeters above the reference ellipsoid as defined by the WGS-84, and is measured to the base of the GNSS antenna.

> Note: FR 3.5.2.4.1 provides the location of the RSU as reported by a GNSS or similar geopositioning device.

3.5.1.1.3.3 Store RSU Location - GNSS Antenna Offset

Upon request from a management station, the RSU shall store the offset in elevation, in centimeters, between the antenna used by a GNSS or similar geopositioning device and the base of the structure that the RSU is mounted on. An RSU determines its geographic location based on data from a GNSS or similar geopositioning device. The geographic position provided by a GNSS (or similar) device is usually based on the location of antenna - the longitude and latitude of the antenna is generally the same location of the RSU, but the height of the antenna is normally higher than the base of the structure. This requirement allows the GNSS data to be adjusted for the height differential.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

3.5.1.1.3.4 Store V2X Antenna Offsets

Upon request from a management station, the RSU shall store the location (latitude, longitude and elevation) of the base of each V2X antenna. The latitude and longitude are in tenths of a microdegree (10^-7 degrees) using the WGS-84 (World Geodetic System 1984). The elevation is in centimeters above the reference ellipsoid as defined by the WGS-84, and is measured to the base of the V2X antenna. The V2X antenna is the antenna for the V2X Radio Interface.

3.5.1.1.3.5 Report Positioning Augmentation

If RSU is receiving geopositioning data from an external GNSS or similar geopositioning device, upon request from a management station, the RSU shall report if its position from the GNSS or similar geopositioning device is augmented with Wide Area Augmentation System (WAAS) corrections.

3.5.1.1.3.6 Forward GNSS Data Requirements

The requirements for the RSU to forward the GNSS data from an external GNSS or similar geopositioning device to another external device follows.

3.5.1.1.3.6.1 Store GNSS Data Output Destination

Upon request from a management station, the RSU shall store the network destination that the RSU forwards the GNSS data from an external GNSS or similar geopositioning device to. The network destination consists of the udp port number, IP address and a text description of the interface.

3.5.1.1.3.6.2 Report GNSS Data Output

Upon request from a management station, the RSU shall report the GNSS data that is being forwarded to an external device.

3.5.1.1.3.6.3 Store GNSS Data Output Interval

Upon request from a management station, the RSU shall store the interval, in seconds, from 1 to 18000 seconds, between transmissions containing the GNSS data to an external device via the network interface (and not across the V2X interface).

3.5.1.1.4 Manage RSU Startup Function Requirements

These requirements allow a transportation manager to configure which configuration file to use and what applications are to be started when the RSU is powered on or rebooted.

3.5.1.1.4.1 Determine Maximum Number of Applications Supported

Upon request by a management station, the RSU shall report the maximum number of applications that can be supported on the RSU.

3.5.1.1.4.2 Manage RSU Startup Functions - Applications

Upon request from a management station, the RSU shall store what applications are part of the RSU's startup functions. This requirement allows the management station to specify which applications are to be started when the RSU is powered on or rebooted. Note that application data exchanges over the V2X interface are identified by PSIDs. Refer to 3.5.1.2.2.1.6.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

3.5.1.1.4.3 Manage RSU Startup Functions - Configuration File

Upon request from a management station, the RSU shall store the name of the configuration file to use as part of the RSU's startup functions. This requirement allows the RSU to be configured for different roles.

3.5.1.1.4.4 Configure Startup Retries

Upon request from a management station, the RSU shall store the allowable number of attempts within a user-defined period to properly reboot an RSU before the RSU enters the 'fault' operating mode. An attempt may be a result of a power up, a reboot, or a watchdog reboot. An RSU fails to properly reboot if the firmware, operating system, or drivers do not load properly during its startup. The 'fault' operating mode (e.g., safe mode) allows the RSU to only load sufficient functionality for a transportation manager to download and install the correct firmware, operating system, drivers and applications without any operational impacts. A value of 0 indicates this feature is disabled (the RSU cannot enter the 'fault' operating mode).

3.5.1.1.4.5 Retrieve Startup Retry Period

Upon request from a management station, the RSU shall retrieve the defined period, in minutes, that an RSU is allowed to attempt reboots before the RSU enters the 'fault' operating mode. The 'fault' operating mode (e.g., safe mode) allows the RSU to only load sufficient functionality for a transportation manager to download and install the correct firmware, operating system, drivers and applications without any operational impacts. The startup retry period is defined by the vendor in consideration of the period of time needed for the RSU to properly start all its required processes.

3.5.1.1.5 Manage RSU Firmware Version Requirements

The requirements to manage the RSU's firmware version follows.

3.5.1.1.5.1 Report the RSU Firmware Version

Upon request from a management station, the RSU shall report the firmware version currently in use by the RSU.

3.5.1.1.5.2 Update the RSU Firmware Version

Upon request from a management station, the RSU shall support firmware updates from an authorized source. The update process allows the transmission of the secure installation files and associated support files for the purpose of the installment of the installation files, and confirmation of a successful update of the RSU firmware.

3.5.1.1.5.3 Report Firmware Update Status

Upon request from a management station, the RSU shall report the status of the process to update the RSU's firmware, and the date and time the status was last updated. The valid values for status are: rejected, roll-backed, processing, successful, and unknown. An attempt to update the firmware may be rejected for a security reason, such as it has not been authenticated. If an attempt to update the firmware fails, the firmware should be roll-backed to the pre-update version.

3.5.1.1.6 Manage Communications Lost Requirements

A communications loss is defined as when a valid communications request has not been received from a management station over a user-specified period of time. The requirements to configure the RSU when communications with the management station is lost follow.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

3.5.1.1.6.1 Configure Short-Term Communications Loss

Upon a request from a management station, the RSU shall store the period of time, in seconds, that communications with the management station is lost to define a short-term communications loss. The short-term communications loss is an event that may result in the RSU changing a behavior, such as to stop broadcasting time-sensitive messages (e.g., traveler information about an unplanned incident). Optionally, the RSU may also have a long-term communications loss event defined. The long-term communications loss duration is greater than the short-term communications loss duration.

3.5.1.1.6.2 Configure Long-Term Communications Loss

Upon a request from a management station, the RSU shall store the period of time, in minutes, that communications with the management station is lost to define a long-term communications loss. The long-term communications loss is an event that may result in the RSU changing a behavior, such as to stop broadcasting messages. Optionally, the RSU may also have a short-term communications loss event defined. The short-term communications loss duration should be less than the long term communications loss duration.

3.5.1.1.6.3 Configure Short-Term Communications Event for Stored Messages

Upon a request from a management station, the RSU shall store what stored messages the RSU is to stop transmitting via the V2X interface when a short term communications loss event occurs. The short-term communications loss event occurs when the period of time since communications was lost with the management station exceeds the short term communications loss duration.

3.5.1.1.6.4 Configure Long-Term Communications Event for Stored Messages

Upon a request from a management station, the RSU shall store what stored messages the RSU is to stop transmitting via the V2X interface when a long term communications loss event occurs. The long term communications loss event occurs when the period of time since communications was lost with the management station exceeds the long term communications loss duration.

3.5.1.1.6.5 Configure Short-Term Communications Event for Immediate Forward Messages

Upon a request from a management station, the RSU shall store if the RSU is to stop transmitting, via the V2X interface, a received message to be forwarded when a short term communications loss event occurs. The short-term communications loss event occurs when the period of time since communications was lost with the management station exceeds the short term communications loss duration.

3.5.1.1.6.6 Configure Long-Term Communications Event for Immediate Forward Messages

Upon a request from a management station, the RSU shall store if the RSU is to stop transmitting, via the V2X interface, a received message for forwarding when a long term communications loss event occurs. The long term communications loss event occurs when the period of time since communications was lost with the management station exceeds the long term communications loss duration.

3.5.1.1.6.7 Configure Long-Term Communications Event for Reboot

Upon a request from a management station, the RSU shall store if the RSU is to reboot when a long term communications loss event occurs. The long term communications loss event occurs when the period of time since communications was lost with the management station exceeds the long term communications loss duration. This requirement allows an operator to avoid a field trip to reboot the RSU in case of a network issue.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

3.5.1.1.7 Manage Notification Requirements

The requirements to configure notifications for the RSU follow.

3.5.1.1.7.1 Store Notification Destination Address

Upon request from a management station, the RSU shall store the destination network address for all notifications generated by the RSU.

3.5.1.1.7.2 Store Notification Destination Port

Upon request from a management station, the RSU shall store the destination port number for all notifications generated by the RSU.

3.5.1.1.7.3 Notification Message Requirements

The requirements for different notification messages for an RSU follow.

3.5.1.1.7.3.1 Notification - Integrity Check Error - Active Message

The RSU shall transmit a notification to the destination network address and port number upon detection of an integrity check error on a message intended to be forwarded to the V2X interface. An integrity check error indicates that the accuracy and consistency of the data in the message may be in doubt. The message may be a stored message intended to be forwarded to the V2X interface for transmission.

3.5.1.1.7.3.2 Notification - Integrity Check Error - Secure Storage

The RSU shall transmit a notification to the destination network address and port number upon detection of an integrity check error on any data parameters in secure storage. An integrity check error indicates that the accuracy and consistency of the data may be in doubt.

3.5.1.1.7.3.3 Notification - Authorization Verification Error

The RSU shall transmit a notification to the destination network address and port number upon detection of an authorization error on any data received by the RSU via the network interface or the V2X interface. An authorization error occurs when the identity of a process or user requesting access to the RSU, its services or its data cannot be authenticated, or if a user, process or application requests a service or data for which it is not authorized.

3.5.1.1.7.3.4 Notification - Signature Verification Error

The RSU shall transmit notifications to the destination network address and port number upon detection of a signature error in the WAVE messages received by the RSU from the V2X interface.

3.5.1.1.7.3.5 Notification - Network Access Control List

The RSU shall transmit a notification to the destination network address and port number upon detection of an attempt of remote network access to the RSU by an application, service, or user from a network address, port number or physical interface not permitted by the RSU's Network Access Control List or Firewall.

3.5.1.1.7.3.6 Notification - Time Source Loss

The RSU shall transmit a notification to the destination network address and port number upon detection of the loss of valid data from the primary time source greater than a defined threshold. The threshold is defined in Sections 3.5.2.3.3 and 3.5.2.3.4.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

3.5.1.1.7.3.7 Notification - Time Source Mismatch

The RSU shall transmit a notification to the destination network address and port number upon detection of a time deviation that exceeds a defined threshold between two time sources. The threshold is defined in Section 3.5.2.3.5.

3.5.1.1.7.3.8 Notification - GNSS Anomaly

The RSU shall transmit a notification to the destination network address and port number upon detection of any spoofing, interference, jamming, or signal integrity discrepancies in the data received from a GNSS or similar geopositioning device.

3.5.1.1.7.3.9 Notification - GNSS Location Deviation

The RSU shall transmit a notification to the destination network address and port number upon detection of a deviation between the RSU's reference location and the geopositioning data received from a GNSS or similar geopositioning device exceeds a defined threshold. See Section 3.5.2.4.3.

3.5.1.1.7.3.10 Notification - Certificate Management

The RSU shall transmit a notification to the destination network address and port number if the RSU has no usable certificates for transmission on the V2X interface or if the certificates are expired.

3.5.1.1.7.3.11 Notification - Denial of Service

The RSU shall transmit a notification to the destination network address and port number if the Channel Busy Ratio on a wireless channel is greater than a user-configurable threshold. The threshold is not defined by NTCIP 1218 v01.

3.5.1.1.7.3.12 Notification - Watchdog

The RSU shall transmit a notification to the destination network address and port number if the watchdog process on the RSU detects a potential fault condition. The watchdog process is a health monitor process on the RSU that monitors all software processes and sets a flag when an application or process appears to be inoperative. The watchdog process may also automatically restart an application or process, or reboot the RSU in the event the watchdog determines a restart or reboot is necessary to restore "normal" operations. An RSU may have more than one watchdog process, one for the main program, and perhaps for each process or service deemed "critical" for the RSU, as determined by the RSU vendor and/or the agency operating the RSU.

3.5.1.1.7.3.13 Notification - GNSS Data

The RSU shall transmit the GNSS data received from a GNSS or similar geopositioning device to the destination network address and port number at user-defined intervals.

3.5.1.1.7.3.14 Notification - Configure GNSS Data Interval

Upon request from a management station, the RSU shall store the interval, in seconds, that the RSU transmits the GNSS data received from a GNSS or similar geopositioning device to.

3.5.1.1.7.3.15 Notification - Environmental

The RSU shall transmit a notification to the destination network address and port number if the RSU detects an environmental error. An environmental error are environmental conditions that may damage

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

the RSU or affect its proper operation. Examples of environmental errors are a high internal temperature which may damage the RSU.

3.5.1.1.7.3.16 Notification - Authentication Failure

The RSU shall transmit a notification to the destination network address and port number if the RSU detects an authentication error from a bad community string (mismatch).

3.5.1.1.7.4 Store Notification Type

Upon request from a management station, the RSU shall store the notification type for each notification message generated by the RSU. The valid values are trap and inform, as defined by snmpNotifyType in RFC 3413. Inform type indicates that the RSU is expecting an acknowledgement that the notification message has been received at the destination address and port.

3.5.1.1.7.5 Store Notification Repeat Intervals

Upon request from a management station, the RSU shall store the minimum period of time, in seconds, required to elapse before re-transmitting a notification message that has not been acknowledged. This requirement is only applicable if the notification message is an inform type, as defined by snmpNotifyType in RFC 3413.

3.5.1.1.7.6 Store Notification Retries

Upon request from a management station, the RSU shall store the maximum number of attempts the RSU is to retransmit a notification message to the destination network address and port number. This requirement is only applicable if the notification message is an inform type, as defined by snmpNotifyType in RFC 3413.

3.5.1.2 Manage Network Interface Requirements

The requirements for the RSU to manage its network interfaces follow.

3.5.1.2.1 Manage a Network Interface Requirements

The requirements for the RSU to manage a network interface follow.

3.5.1.2.1.1 Enable/Disable a Communications Port

Upon request from a management station, the RSU shall enable or disable a communications port on the RSU.

3.5.1.2.1.2 Configure Ethernet Ports

Upon request from a management station, the RSU shall store the network address, gateway address, subnet mask and whether DHCP is enabled for an Ethernet port on the RSU.

3.5.1.2.1.3 Report Ethernet Port - MAC Address

Upon request from a management station, the RSU shall report the MAC address for an Ethernet port on the RSU.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

3.5.1.2.2 Message Management Requirements

The requirements for the RSU to manage messages that are to be transmitted over the V2X interface follow.

3.5.1.2.2.1 Manage Stored Message Requirements

The requirements for the RSU to manage messages stored on the RSU follow.

3.5.1.2.2.1.1 Determine Maximum Number of Stored Messages Supported

Upon request by a management station, the RSU shall report the maximum number of messages that can be stored on the RSU for future transmission.

3.5.1.2.2.1.2 Store a Message

Upon request by a management station, the RSU shall store a message for future transmission.

3.5.1.2.2.1.3 Delete a Stored Message

Upon request by a management station, the RSU shall delete a message from its storage.

3.5.1.2.2.1.4 Enable/Disable the Transmission of a Stored Message

Upon request by a management station, the RSU shall store if a stored message is enabled or disabled for transmission.

3.5.1.2.2.1.5 Store a Message Type

Upon request by a management station, the RSU shall store the message type of a stored message. The message type is identified by the DE_DSRC_MessageID data element, as defined in SAE J2735_201603.

3.5.1.2.2.1.6 Store PSID for Application Data Exchanges

Upon request by a management station, the RSU shall store the PSID that identifies an application data exchange over the V2X interface.

3.5.1.2.2.1.7 Delete All Stored Messages

Upon request by a management station, the RSU shall delete all stored messages from the RSU's memory. This requirement allows a transportation manager to clear all stored messages prior to field installation or for testing purposes.

3.5.1.2.2.1.8 Store a Message's Priority

Upon request by a management station, the RSU shall store the user priority assigned to a stored message. For a V2X radio, the user priority is an integer value and is defined in IEEE 1609.3-2016.

3.5.1.2.2.1.9 Store a Message's Transmission Interval

Upon request by a management station, the RSU shall store the time interval, in milliseconds, between successive transmissions that a stored message is to be transmitted.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

3.5.1.2.2.1.10 Store a Message's Transmission Channel

Upon request by a management station, the RSU shall store the transmission channel, as defined by the appropriate regulatory domain, a stored message is to be transmitted on. The valid values for the transmission channel are 0 to 255.

Note: For radios using IEEE 802.11, the transmission channel number is defined by IEEE 802.11-2016. For PC5 radios, the equivalent transmission channel number is defined in Table 7, where EARFCN is the E-UTRA Absolute Radio Frequency Channel Number.

Table 7 3GPP Channel Number Mapping to IEEE 802.11 Channel Number

Channel Number (See IEEE 802.11)	Center Frequency (MHz)	Bandwidth	EARFCN (3GPP Channel Number)
172	5860	10 MHz	54590
174	5870		54690
176	5880		54790
178	5890		54890
180	5900		54990
182	5910		55090
184	5920		55190
173	5865	20 MHz	54640
175	5875		54740
177	5885		54840
179	5895		54940
181	5905		55040
183	5915		55140

Figure 6 is a graphical depiction of the IEEE 802.11 channel mappings.

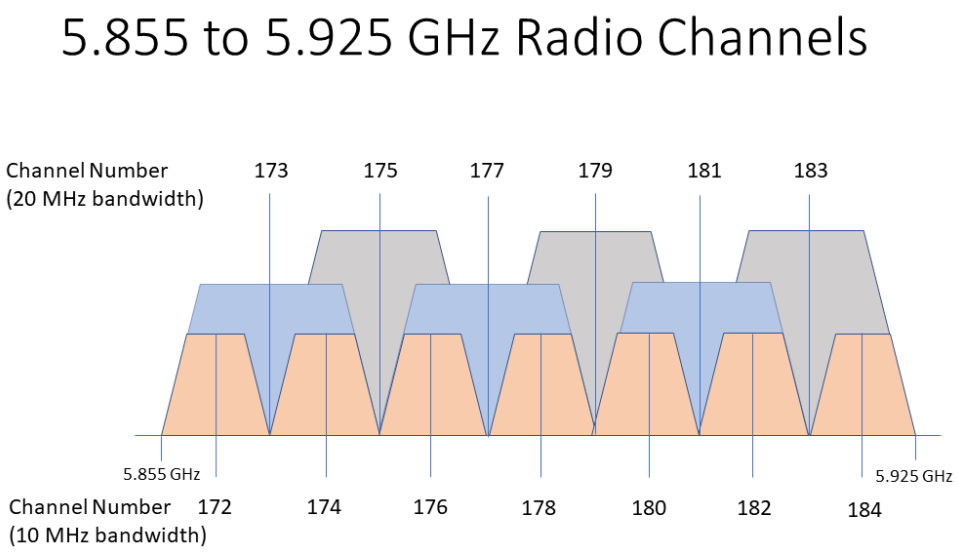

Figure 6 IEEE 802.11 Channel Number Mapping

Note: For DSRC in the United States at the time of publication, the transmission channel is a value from 172 to 184, inclusive, as defined by FCC 47 C.F.R., Part 90.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

3.5.1.2.2.1.11 Store a Message's Transmission Start Time

Upon request by a management station, the RSU shall store the start date and time that a stored message is to begin transmission.

3.5.1.2.2.1.12 Store a Message's Transmission Stop Time

Upon request by a management station, the RSU shall store the stop date and time that a stored message is to end transmission.

3.5.1.2.2.1.13 Store if a Message is to be Signed

Upon request by a management station, the RSU shall store if the payload of the stored message is to be signed prior to forwarding the message for transmission to the V2X wireless interface. A RSU has three options for signing the payload of a stored message: sign, which is to sign and wrap the message into an appropriate security header; do-not-sign, which still wraps the message into a security header but without signing the message; and bypass, which transmits the payload "as-is" without even wrapping the message into a security header. This last option assumes that the transmitter of the payload already put the appropriate security header into the payload.

3.5.1.2.2.2 Manage Immediate Forward Message Requirements

The requirements for the RSU to manage messages received by the RSU for immediate transmission over the V2X interface follow.

3.5.1.2.2.2.1 Determine Maximum Number of Immediate Forward Messages Supported

Upon request by a management station, the RSU shall report the maximum number of message types received for forwarding that can supported on the RSU.

3.5.1.2.2.2.2 Forward Message to the V2X Interface

Upon request by a management station, the RSU shall store a received message to be forwarded immediately to the V2X interface for transmission. The received message shall be authenticated and from a trusted source, such as an SNMPv3 OID.

3.5.1.2.2.2.3 Store the Message Type for a Message for Forwarding to the V2X Interface

Upon request by a management station, the RSU shall store the message type of a message received for forwarding to the V2X interface for transmission. The message type is identified by the DE_DSRC_MessageID data element, as defined in SAE J2735_201603.

3.5.1.2.2.2.4 Store the PSID for an Application Data Exchange for Forwarding to the V2X Interface

Upon request by a management station, the RSU shall store the PSID for an application data exchange received for forwarding to the V2X interface for transmission.

3.5.1.2.2.2.5 Store the Priority for a Message for Forwarding to the V2X Interface

Upon request by a management station, the RSU shall store the user priority assigned for a message received for forwarding to the V2X interface for transmission. For a V2X radio, the user priority is an integer value and is defined in IEEE 1609.3-2016.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

3.5.1.2.2.2.6 Store the Transmission Channel for a Message for Forwarding to the V2X Interface

Upon request by a management station, the RSU shall store the transmission channel, as defined by the appropriate regulatory domain, that a received message for forwarding to the V2X interface is to be transmitted on. The valid values for the transmission channel are 0 to 255.

> Note: For radios using IEEE 802.11, the transmission channel number is defined by IEEE 802.11-2016. For PC5 radios, the equivalent transmission channel number is defined in Table 7, where EARFCN is the E-UTRA Absolute Radio Frequency Channel Number.
>
> Note: For DSRC in the United States at the time of publication, the transmission channel is a value from 172 to 184, inclusive, as defined by FCC 47 C.F.R., Part 90.

3.5.1.2.2.2.7 Store if a Received Message for Forwarding to the V2X Interface is Signed

Upon request by a management station, the RSU shall store if the payload of a received message is to be signed prior to forwarding the message for transmission to the V2X interface. A RSU has three options for signing the payload of a received message for forwarding: sign, which is to sign and wrap the message into an appropriate security header; do-not-sign, which still wraps the message into a security header but without signing the message; and pass-through, which transmits the payload "as-is" without even wrapping the message into a security header. This last option assumes that the transmitter of the payload already put the appropriate security header into the payload.

3.5.1.2.2.3 Manage Messages Received from the V2X Interface Requirements

The requirements for the RSU to manage messages received by the RSU over the V2X interface follow.

3.5.1.2.2.3.1 Determine Maximum Number of Message Received Types Supported

Upon request by a management station, the RSU shall report the maximum number of message types and message destinations for forwarding that can supported on the RSU.

3.5.1.2.2.3.2 Store Network Destination to Forward Messages Received from the V2X Interface

Upon request by a management station, the RSU shall store the network address and port number that all messages received from the V2X interface with a specified PSID are to be forwarded to. A message with a specified PSID may be forwarded to more than one network address and port number.

3.5.1.2.2.3.3 Store Transport Protocol to Forward Messages Received from the V2X Interface

Upon request by a management station, the RSU shall store the transport protocol to use to forward all messages received from the V2X interface with a specified PSID to a specified network address and port number.

3.5.1.2.2.3.4 Store Minimum Signal Strength to Forward Messages Received from the V2X Interface

Upon request by a management station, the RSU shall store the minimum received signal strength indication (RSSI) level of the message received from the V2X interface with a specified PSID, before forwarding the message to a specified network address and port number. Valid RSSI levels are from -100 to -60 dbm in units of 1 dbm.

3.5.1.2.2.3.5 Store Message Interval to Forward Messages Received from the V2X Interface

Upon request by a management station, the RSU shall store the message interval for forwarding messages received from the V2X interface with a specified PSID to a specified network address and port

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

number. This requirement forwards every Nth message received by the V2X interface meeting all the specified criteria (PSID, RSSI) to the specified network address and port number. Valid values for n are from 1 to 9, with 1 indicating that all messages are to be forwarded.

3.5.1.2.2.3.6 Store Start Time to Forward Messages Received from the V2X Interface

Upon request by a management station, the RSU shall store the start date and time that messages received from the V2X interface with a specified PSID are to be forwarded to a specified network address and port number.

3.5.1.2.2.3.7 Store Stop Time to Forward Messages Received from the V2X Interface

Upon request by a management station, the RSU shall store the stop date and time that messages received from the V2X interface with a specified PSID are to stop being forwarded to a specified network address and port number.

3.5.1.2.2.3.8 Enable/Disable Forwarding Messages Received from the V2X Interface

Upon request by a management station, the RSU shall store if messages received from the V2X interface with a specified PSID are to be forwarded to a specified network address and port number.

3.5.1.2.2.3.9 Store Secure Options to Forward Messages Received from the V2X Interface

Upon request by a management station, the RSU shall store if only the payload content of the messages received from the V2X interface are forwarded to a specified network address and port number. This requirement allows the RSU is to strip any certificates and signatures from the message before forwarding the payload content.

3.5.1.2.2.3.10 Store Interval to Authenticate Messages Received from the V2X Interface

Upon request by a management station, the RSU shall store the interval for authenticating messages received from the V2X interface with a specified PSID to a specified network address and port number and marked for forwarding. This requirement instructs the RSU to check the certificate and signature of every Nth message received by the V2X interface meeting all the specified criteria (PSID, RSSI) to the specified network address and port number and marked for forwarding (See 3.5.1.2.2.3.5). Valid values for n are from 1 to 9, with 1 indicating that all messages are to be forwarded. A value of 0 indicates that authentication is disabled.

3.5.1.2.2.4 Forward Messages Transmitted Over the V2X Interface Requirements

The requirements for the RSU to forward to a specified network destination messages transmitted over the V2X interface follow.

3.5.1.2.2.4.1 Determine Maximum Number of Message Entries Transmitted Over the V2X Interface For Forwarding Supported

Upon request by a management station, the RSU shall report the maximum number of message types transmitted over the V2X interface and message destinations for forwarding that can supported on the RSU.

3.5.1.2.2.4.2 Store Network Destination to Forward Messages Transmitted Over the V2X Interface

Upon request from a management station, the RSU shall store the network destination that the RSU forwards the messages that have been transmitted over the V2X interface with a specified PSID. The network destination consists of the IP address, the port number and a text description of the interface.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

3.5.1.2.2.4.3 Store Transport Protocol to Forward Messages Transmitted Over the V2X Interface

Upon request from a management station, the RSU shall store the transport protocol to use to forward the messages that have been transmitted over the V2X interface with a specified PSID.

3.5.1.2.2.4.4 Store Start Time to Forward Messages Transmitted Over the V2X Interface

Upon request by a management station, the RSU shall store the start date and time that messages transmitted over the V2X interface with a specified PSID are to be forwarded to a specified network address and port number.

3.5.1.2.2.4.5 Store Stop Time to Forward Messages Transmitted Over the V2X Interface

Upon request by a management station, the RSU shall store the stop date and time that messages transmitted over the V2X interface with a specified PSID are to stop being forwarded to a specified network address and port number.

3.5.1.2.3 Logging of Interface Data Requirements

The requirements to manage the interface data logs for the RSU follow.

3.5.1.2.3.1 Determine Maximum Number of Interface Logs Supported

Upon request by a management station, the RSU shall report the maximum number of active interface logs that can supported on the RSU.

3.5.1.2.3.2 Log Interface Data Identification

Upon request from a management station, the RSU shall store a list of interfaces for which the RSU shall log all transmitted and received packets.

3.5.1.2.3.3 Log Interface Data by Direction

Upon request from a management station and if the RSU is logging packets, the RSU shall generate separate log files for transmitted and received packets across a specified interface.

3.5.1.2.3.4 Store Interface Data Log - File Directory

Upon request from a management station, the RSU shall store the interface data logs in a specified directory on the RSU.

3.5.1.2.3.5 Retrieve Interface Logged Data

Upon request from a management station, the RSU shall return the logged data in the interface data log.

3.5.1.2.3.6 Store an Interface Data Log Start Time

Upon request by a management station, the RSU shall store the start date and time to begin logging data packets across a specified interface.

3.5.1.2.3.7 Store an Interface Data Log Stop Time

Upon request by a management station, the RSU shall store the stop date and time to stop logging data packets across a specified interface.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

3.5.1.2.3.8 Store Maximum Interface Data Log File Size

Upon request from a management station, the RSU shall store the maximum file size supported by the RSU for an interface data log, in megabytes, from 1 to 40 megabytes. The RSU is to open a new interface data log file when an active interface data log reaches this maximum interface data log file size. This requirement allows the transportation manager to determine if there is sufficient space to continue storing interface data logs without crashing the RSU.

3.5.1.2.3.9 Store Maximum Interface Data Log File Collection Time

Upon request from a management station, the RSU shall store the minimum collection time supported by the RSU for an interface data log, in hours, from 1 to 48 hours. The RSU is to open a new interface data log file when an active interface data log reaches this maximum interface data log time.

3.5.1.2.3.10 Store Interface Data Log Option - Disk Full

Upon request from a management station, the RSU shall store if the RSU is to stop interface data logging or delete the oldest interface data log file is the disk space available for interface data logs is full.

3.5.1.2.3.11 Store Interface Data Log Option - Entry Deletion

Upon request from a management station, the RSU shall store if the RSU is to delete the interface data log file when its interface data log entry is deleted. It is assumed that a transportation manager retrieves the interface data log file from the RSU before deleting the interface data log entry from the RSU.

3.5.1.3 Configure V2X Interfaces Requirements

The requirements to configure the V2X interface for the RSU follow.

3.5.1.3.1 Configure Radio Requirements

The requirements to configure the radios associated with the V2X interface for an RSU follow.

3.5.1.3.1.1 Report Maximum Number of V2X Radios Supported

Upon request from a management station, the RSU shall report the maximum number of V2X radios supported by the RSU identity and version of the MIB(s) in use.

3.5.1.3.1.2 Report Type of V2X Radio

Upon request from a management station, the RSU shall report the type of V2X radios managed by the RSU. Valid values are dsrc and PC5.

3.5.1.3.1.3 Enable/Disable Radios

Upon request from a management station, the RSU shall enable or disable a V2X radio managed by the RSU. This requirement allows a transportation manager to stop the radio from broadcasting and receiving messages.

3.5.1.3.1.4 Report Radio MAC Address

Upon request from a management station, the RSU shall report the IEEE 802.11 MAC address of each V2X radio managed by the RSU. If the V2X interface is DSRC, it reports the MAC address; if the V2X radio is PC5, it reports the radio index (i.e. radio 1, radio 2, etc.).

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

3.5.1.3.1.5 Report Radio Operating Modes

Upon request from a management station, the RSU shall report if its V2X radios are operating in continuous or alternating modes.

3.5.1.3.2 Determine Lower Layer Requirements

The requirements to report the lower layer parameters associated with the V2X interface for an RSU follow.

3.5.1.3.2.1 Determine Lower Layer Parameter

Upon request from a management station, if the V2X radio is a DSRC interface, the RSU shall report an enhanced distributed channel access (EDCA) parameter set for a V2X radio. The EDCA parameter set consists of, as defined in IEEE 802.11-2016, the Arbitration Interframe Spacing (AIFSN), Contention Window Minimum Value (CWmin), Contention Window Maximum Value (CWmax), and the Transmission Opportunity (TXOP) limit.

3.5.1.3.2.2 Determine Operating Class

Upon request from a management station, the RSU shall report the operating class, as defined in IEEE 802.11 or media used, that a V2X radio is configured for. Valid values for the operating class are from 0 to 255.

3.5.1.3.3 Configure IEEE 1609 Communications Requirements

The requirements to configure the IEEE 1609 parameters for the RSU follow.

3.5.1.3.3.1 Manage IEEE 1609.2 Security Requirements

Upon request from a management station, the RSU shall obtain and manage IEEE 1609.2 certificates to sign and encrypt messages for transmission via the radio. An RSU is expected to have two types of certificates, enrollment certificates and application certificates. Enrollment certificates are handled by the RSU manufacturer and contains the domain name URL where the application certificates would come from. The requirements to configure IEEE 1609.2 certificates for the RSU follow.

3.5.1.3.3.1.1 Report IEEE 1609.2 Enrollment Certificate - Status

Upon request from a management station, the RSU shall report the status of the enrollment certificates. The valid values are notEnrolled, enrolled, unknown and other.

3.5.1.3.3.1.2 Report IEEE 1609.2 Enrollment Certificate - Expiration Date

Upon request from a management station, the RSU shall report the expiration date of the enrollment certificates.

3.5.1.3.3.1.3 Report IEEE 1609.2 Enrollment Certificate - Source Domain

Upon request from a management station, the RSU shall report the domain uniform resource locator (URL) of the Certificate Authority that is the source of the enrollment certificate.

3.5.1.3.3.1.4 Report IEEE 1609.2 Enrollment Certificate Identifier

Upon request from a management station, the RSU shall report the enrollment certificate identifier.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

3.5.1.3.3.1.5 Report IEEE 1609.2 Enrollment Certificate - Valid Region

Upon request from a management station, the RSU shall report a region identifier, such as a country code, that the enrollment certificate is valid for. For the United States, the valid region identifier is the country code, 840.

3.5.1.3.3.1.6 Report IEEE 1609.2 Enrollment Certificate - Source

Upon request from a management station, the RSU shall report if the source of the enrollment certificates is the Security Credential Management System (SCMS) or the certificates were manually loaded (obtained).

3.5.1.3.3.1.7 Report IEEE 1609.2 Application Certificates - Status

Upon request from a management station, the RSU shall report the status of the application certificates. The valid values are valid, processing, failed, expired, and unknown.

3.5.1.3.3.1.8 Report IEEE 1609.2 Application Certificates - Source

Upon request from a management station, the RSU shall report the domain uniform resource locator (URL) from which to request new application certificates.

3.5.1.3.3.1.9 Store IEEE 1609.2 Application Certificates - Default Request Interval

Upon request from a management station, the RSU shall store the default interval, in hours, between new requests for application certificates.

3.5.1.3.3.1.10 Store IEEE 1609.2 Application Certificates - Request Interval

Upon request from a management station, the RSU shall store the interval, in hours, between new requests for application certificates for a specified PSID.

3.5.1.3.3.1.11 Report Certificate Revocation List - Source

Upon request from a management station, the RSU shall report the domain name URL from which to request updated certificate revocation lists.

3.5.1.3.3.1.12 Report Certificate Revocation List - Update Time

Upon request from a management station, the RSU shall report the date and time the certificate revocation list was last updated.

3.5.1.3.3.1.13 Store Certificate Revocation List Update Interval

Upon request from a management station, the RSU shall store the interval, in hours, between requests for an updated certificate revocation list.

3.5.1.3.3.1.14 Update Certificate Revocation List Command

Upon request from a management station, the RSU shall make a request to update its certificate revocation list from the certificate authority.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

3.5.1.3.3.1.15 Report IEEE 1609.2 Security Profiles

Upon request from a management station, the RSU shall report the name and description of the IEEE 1609.2 security profile for a PSID stored on the RSU. A security profile proforma is defined in IEEE 1609.2-2016.

3.5.1.3.3.2 Configure IEEE 1609.3 Communications - WSA Requirements

The requirements to configure the WAVE Service Advertisement (WSA) for the RSU follow. Broadcast messages from a V2X radio are not required to be preceded by or associated with a WSA. Note that the WSA is identified as an application that has a unique PSID and potentially a unique certificate. Refer to 3.5.1.3.3.1 for application certificate requirements.

3.5.1.3.3.2.1 Determine Maximum Number of Services Advertised

Upon request by a management station, the RSU shall report the maximum number of PSIDs that can be advertised by the RSU.

3.5.1.3.3.2.2 Store WSA Configuration - Service Info Segment

Upon request from a management station, the RSU shall store a service info segment for a WSA. A service info segment for a WSA is defined in IEEE 1609.3-2016 and provides information about a service, which is usually an application that is advertised by and accessible from or through the RSU. A service info segment consists of the PSID; the Provider Service Context (PSC) information; the IPv6 address, port number and provider MAC address used to access the application service; the RCPI threshold; the WSA count threshold, WSA count threshold interval, and if the service is a routed service. All elements in the service info segment are optional except the PSID. Note that a WSA is not required to support broadcast messages.

3.5.1.3.3.2.3 Store WSA Configuration - Channel Info Segment

Upon request from a management station, the RSU shall store the desired transmission information for a service provided by the RSU. The transmission information consists of the operating class, the transmission channel (number) to advertise the service, the transmit power level to be used, and the transmission interval for the advertisement. The RSU uses this information to advertise services on the appropriate transmission channels, power levels and intervals.

3.5.1.3.3.2.4 Configure WSA Configuration - WAVE Router Advertisement

Upon request from a management station, the RSU shall configure a WAVE router advertisement (WRA) segment for a WSA. A WRA segment for a WSA is defined in IEEE 1609.3-2016 and provides information to configure an IPv6 interface so messages received from a connected device via the V2X can be immediately exchanged with a remote host. A WRA contains the network address of the remote host, the network gateway, the primary Domain Name System (DNS), and optionally the network address of the secondary DNS and gateway MAC address.

3.5.1.3.3.2.5 Store WSA Configuration - Secure

Upon request from a management station, the RSU shall report whether the WSA transmitted over the V2X interface are to be secure (signed) or unsecure.

3.5.1.3.3.2.6 Report WSA Version Number

Upon request from a management station, the RSU shall report the WSA Version Number, as defined in IEEE 1609.3-2016, used by the RSU.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

3.5.1.3.3.3 Configure IEEE 1609.4 Communications Requirements

The requirements to configure the RSU for multi-channel operations follow. These requirements apply only to DSRC radios.

3.5.1.3.3.3.1 Store the IEEE 1609.4 Configuration for a Radio

Upon request from a management station, the RSU shall store the parameters for a radio. The parameters consist of a textual description of the radio, the service channel and the transmission channels the radio operates on as defined by the appropriate regulatory domain. The valid values for the transmission channels are 0 to 255.

> Note: For radios using IEEE 802.11, the transmission channel number is defined by IEEE 802.11-2016. For PC5 radios, the equivalent transmission channel number is defined in Table 7, where EARFCN is the E-UTRA Absolute Radio Frequency Channel Number.
>
> Note: For DSRC in the United States at the time of publication, the transmission channel is a value from 172 to 184, inclusive, as defined by FCC 47 C.F.R., Part 90.

3.5.1.3.3.3.2 Store Radio Channel Access Mode

Upon request from a management station, the RSU shall store the channel access options (continuous, alternating, immediate) of the radio, and if the immediate or extended option for channel switching is used (if applicable). The valid values for channel access options are continuous, alternating, immediate, other and unknown.

3.5.1.3.4 Configure V2X Radio Transmitter Requirements

The requirements to configure the radio transmitter properties associated with the V2X interface for an RSU follow.

3.5.1.3.4.1 Store Default Transmit Power

For a message with a specified PSID forwarded to a radio for transmission, upon request from a management station, the RSU shall report the default transmit power level, in dBm, at the antenna port to be used for transmission for a channel. The valid range for the default power is from -128 to 127 dBm, in units of 1 dBm.

> Note: The default transmit power could be dynamic and changed by channel or an application.

3.5.1.3.4.2 Report Maximum Number of V2X Antennas Supported

Upon request from a management station, the RSU shall report the maximum number of V2X antennas supported by the RSU.

3.5.1.3.4.3 Store Antenna Gain and Cable Losses

Upon request from a management station, the RSU shall store the antenna gain for a radio antenna, in units of 0.01 dB. This requirement is applicable if the antenna is not direct connect.

3.5.1.3.4.4 Store Antenna Type

Upon request from a management station, the RSU shall store the direction that the antenna is pointing at along the horizontal plane. A value of 360 indicates uniform gain in all directions in the horizontal plane.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

3.5.1.4 Manage RSU Applications Requirements

The requirements for managing the applications on the RSU follow.

3.5.1.4.1 Manage RSU Application Requirements

The requirements for managing an application on the RSU follow.

3.5.1.4.1.1 Install an RSU Application

Upon request from a management station, an RSU shall support the installation of new or updated software from an authorized source. The installation process allows the transmission of the secure installation files, executable application code and associated support files to support the installation files, and confirmation of a successful update of the software.

Note: The expectation is that the management station loads the installation files to the RSU.

3.5.1.4.1.2 Report Software Update Status

Upon request from a management station, the RSU shall report the status of the process to install software, and the date and time the status was last updated. The valid values for status are: rejected, roll-backed, processing, successful, and unknown. An attempt to update the software may be rejected for a security reason, such as it has not been authenticated. If applicable, if an attempt to update the software fails, the software should be roll-backed to the pre-update version.

3.5.1.4.2 Manage RSU Application Configuration Requirements

The requirements for managing the configuration of an application on the RSU follow.

3.5.1.4.2.1 Install a Configuration File

Upon request from a management station, an RSU shall begin the installation of a configuration file from an authorized source. The installation allows the transmission of the secure installation files and associated support files to support the installation files, and confirmation of a successful update of the application or process.

3.5.1.4.2.2 Report Configuration File Update Status

Upon request from a management station, the RSU shall report the status of the process to install an updated configuration file, and the date and time the status was last updated. The valid values for status are: rejected, roll-backed, processing, successful, and unknown. An attempt to update the configuration file may be rejected for a security reason, such as it has not been authenticated. If an attempt to update the configuration file fails, the configuration file should be rolled-back to the pre-update version.

3.5.1.5 Manage Location Corrections Requirements

The requirements for managing location corrections data provided by the RSU follow.

3.5.1.5.1 Forward Location Corrections Data

Upon request from a management station, the RSU shall forward location corrections data received from an external source for transmission via the V2X interface. Examples of location corrections data are RTCM Corrections messages as recommended in SAE J2945_201712 and SAE J2735_201603.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

3.5.1.5.2 Use RTCM Corrections Data

Upon request from a management station, the RSU shall receive and transmit the RTCM SC-104 Corrections messages received from a validated external source.

3.5.2 RSU Monitoring Requirements

The requirements for monitoring the operation of the RSU device follow.

3.5.2.1 Determine RSU Operational Performance Status Requirements

The requirements for monitoring the operational performance for the RSU follow.

3.5.2.1.1 Report Time Elapsed Since RSU Power On

Upon request from a management station, the RSU shall report the amount of time that has elapsed since it has been powered on, in seconds.

3.5.2.1.2 Report Amount of Free Memory

Upon request from a management station, the RSU shall report the amount of free volatile memory, in megabytes, available on the RSU.

3.5.2.1.3 Report Instantaneous CPU Load

Upon request from a management station, the RSU shall report the CPU load of the RSU at the time of the request, in percent, from 0 to 100 percent.

3.5.2.1.4 Report CPU Load Average - 15 Minutes

Upon request from a management station, the RSU shall report the average CPU load of the RSU for the previous 15 minutes, in percent, from 0 to 100 percent.

3.5.2.1.5 Report CPU Load Average - 5 Minutes

Upon request from a management station, the RSU shall report the average CPU load of the RSU for the previous 5 minutes, in percent, from 0 to 100 percent.

3.5.2.1.6 Report CPU Load Average - 1 Minute

Upon request from a management station, the RSU shall report the average CPU load of the RSU for the previous minute, in percent, from 0 to 100 percent.

3.5.2.1.7 Report Storage Space Available

Upon request from a management station, the RSU shall report the amount of non-volatile available storage space, in megabytes. The storage space in the RSU may be used to store interface data logs, applications, etc.

3.5.2.1.8 Report Number of Messages Exchanged

Upon request from a management station, the RSU shall report the number of messages transmitted and received over the V2X interface, sorted by channel and direction (transmitted or received), since the RSU was last rebooted or since the time the RSU was commanded to begin tracking the number of messages exchanged.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

3.5.2.2 Report Mode of Operations

Upon request from a management station, the RSU shall report the current mode of operation of the RSU. Valid values are standby, operate, and fault.

In 'standby' mode, the RSU's V2X radio is not enabled and interface logging is disabled.

The RSU is in 'operate' mode when V2X radio is enabled (transmitting and receiving), system logging is enabled, and periodic communications with a management station (e.g., an operations center) is enabled.

In 'fault' mode, the RSU is not fully functional, only minimally responsive and is not transmitting messages over the V2X interface. For example, the RSU may enter fault mode if the RSU fails to properly reboot (e.g., all system drivers or firmware properly start) after a configurable number of attempts.

3.5.2.3 Determine RSU Clock Status Requirements

The requirements for managing the clock of an RSU follow.

3.5.2.3.1 Report RSU Clock Source

Upon request from a management station, the RSU shall report the primary clock source for the RSU. The valid values are crystal, GNSS, NTP, and other.

3.5.2.3.2 Report RSU Clock Status

Upon request from a management station, the RSU shall report the status of the system clock in the RSU. The valid values are active and pending update.

3.5.2.3.3 Store Allowable RSU Clock Source Timeout

Upon request from a management station, the RSU shall store a timeout value, from 1 to 3600 seconds, representing the allowable amount of time that communications from the primary time source may be lost.

3.5.2.3.4 Store Allowable RSU Clock Source Queries

Upon request from a management station, the RSU shall store the number of allowable consecutive failed query attempts, from 1 to 15, for time information from the primary time source.

3.5.2.3.5 Store Allowable Time Deviation

Upon request from a management station, the RSU shall store the allowable deviation, in milliseconds, between two or more time sources.

3.5.2.4 Determine RSU Location Requirements

The requirements for the RSU to determine its location information follow.

3.5.2.4.1 Report RSU Location

Upon request from a management station, the RSU shall return its current location as reported by a GNSS or similar geopositioning device. The RSU location consists of the latitude, longitude, and elevation. The latitude and longitude are measured in tenths of a microdegrees (10^-7 degrees) based on the WGS-84 (World Geodetic System 1984). The elevation of the RSU is in centimeters above the reference ellipsoid as defined by WGS-84, and is measured to the base of the GNSS antenna.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

3.5.2.4.2 Report Positioning Status

Upon request from a management station, the RSU shall return the number of satellites, from 0 to 15, the GNSS or similar geopositioning device is tracking.

3.5.2.4.3 Store Allowable RSU Location Tolerance

Upon request from a management station, the RSU shall store the maximum allowable tolerance, in centimeters, between the last location reported by a GNSS or similar geopositioning device and the RSU's reference location. The tolerance is reported as the distance between the two coordinates (longitude and latitude), from 1 to 20,000 meters. This requirement is used by the RSU to determine if a notification should be transmitted to a management station.

3.5.2.4.4 Report RSU Location Deviation

Upon request from a management station, the RSU shall report the deviation, in centimeters, between the location reported by a GNSS or similar geopositioning device and the RSU's reference location.

3.5.2.4.5 Report RSU Estimated Location Error

Upon request from a management station, the RSU shall report the estimated location error the GNSS or similar geopositioning device is experiencing. The estimated location error is defined along the semi-major axis, semi-minor axis, and orientation, as defined by DF_PositionalAccuracy in SAE J2735_201603.

3.5.2.5 Monitor Network Interface Requirements

The requirements for the RSU to monitor its network interfaces follow.

3.5.2.5.1 Monitor Data Link Errors - Ethernet

Upon request from a management station, the RSU shall return the number of the communications errors that have occurred on an Ethernet port. Communications errors include a bad CRC and framing errors resulting in a corrupted message.

3.5.2.6 Report Number of Messages Exchanged by V2X Radio and PSID

Upon request by a management station, the RSU shall report the number of messages transmitted and received by the RSU, sorted by PSID and V2X radio, over the radio since the RSU was last powered on or the RSU was rebooted. If the application is IP-based, the RSU stores the number of messages comprising the entire corresponding data exchange.

3.5.2.7 Determine Number of Active Radios

Upon request from a management station, the RSU shall report the number of active radios associated with the RSU used for the V2X Interface. Valid values are from 0 to 7, with a value for unknown.

3.5.2.8 Determine RF Communications Range Requirements

Requirements to determine the effective RF communications range for V2X communications around the RSU follow.

3.5.2.8.1 Determine Maximum Number of Communications Range Entries

Upon request by a management station, the RSU shall report the maximum number of communications range entries that can be supported on the RSU. Each entry represents the communications range

 © 2020 AASHTO / ITE / NEMA

statistics based on a message type, a vehicle type or vehicle class, and one or more sixteen 22.5 degree sectors.

3.5.2.8.2 Report the RF Communications Distance - 1 Minute

Upon request from a management station, the RSU shall report the farthest distance, in meters, from the location of the RSU by sector that a message was received via the V2X interface over the previous 1 minute by message type and vehicle type. This requirement allows an RSU to determine the radio coverage in each of sixteen 22.5 degree sectors around the RSU. The first sector starts from North and ends at 22.5 degrees from North in an eastward direction and the distance is measured in tenths of a meter. The message type is identified by the DE_DSRC_MessageID data element, as defined in SAE J2735_201603. The vehicle type is defined by DE_VehicleType, as defined in SAE J2735_201603, which represents the FHWA 13-Vehicle Category Classification. A distance of 0 meters indicates no messages are received.

3.5.2.8.3 Report the RF Communications Distance - 5 Minutes

Upon request from a management station, the RSU shall report the farthest distance, in meters, from the location of the RSU by sector that a message was received via the V2X interface over the previous 5 minutes by message type and vehicle type. This requirement allows an RSU to determine the radio coverage in each of sixteen 22.5 degree sectors around the RSU. The first sector starts from North and ends at 22.5 degrees from North in an eastward direction and the distance is measured in tenths of a meter. The message type is identified by the DE_DSRC_MessageID data element, as defined in SAE J2735_201603. The vehicle type is defined by DE_VehicleType, as defined in SAE J2735_201603, which represents the FHWA 13-Vehicle Category Classification. A distance of 0 meters indicates no messages are received.

3.5.2.8.4 Report the RF Communications Distance - 15 Minutes

Upon request from a management station, the RSU shall report the farthest distance, in meters, from the location of the RSU by sector that a message was received via the V2X interface over the previous 15 minutes by message type and vehicle type. This requirement allows an RSU to determine the radio coverage in each of sixteen 22.5 degree sectors around the RSU. The first sector starts from North and ends at 22.5 degrees from North in an eastward direction and the distance is measured in tenths of a meter. The message type is identified by the DE_DSRC_MessageID data element, as defined in SAE J2735_201603. The vehicle type is defined by DE_VehicleType, as defined in SAE J2735_201603, which represents the FHWA 13-Vehicle Category Classification. A distance of 0 meters indicates no messages are received.

3.5.2.8.5 Report the Average RF Communications Distance - 1 Minute

Upon request from a management station, the RSU shall report the average farthest distance from the location of the RSU by sector from which a message was received via the V2X interface over the previous 1 minute by message type and vehicle type. This requirement assumes that the RSU has the ability to determine when a mobile device is first or last detected by the RSU within a sector. This calculation is a simple average of the location of each mobile device detected by the RSU in the previous 1 minute. This requirement allows an RSU to determine the radio coverage in each of sixteen 22.5 degree sectors around the RSU. The first sector starts from North and ends at 22.5 degrees from North in an eastward direction and the distance is measured in tenths of a meter. The message type is identified by the DE_DSRC_MessageID data element, as defined in SAE J2735_201603. The vehicle type is defined by DE_VehicleType, as defined in SAE J2735_201603, which represents the FHWA 13-Vehicle Category Classification. A distance of 0 meters indicates no messages are received.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

3.5.2.8.6 Report the Average RF Communications Distance - 5 Minutes

Upon request from a management station, the RSU shall report the average farthest distance from the location of the RSU by sector from which a message was received via the V2X interface over the previous 5 minutes by message type and vehicle type. This requirement assumes that the RSU has the ability to determine when a mobile device is first or last detected by the RSU within a sector. This calculation is a simple average of the location of each mobile device detected by the RSU in the previous 5 minutes. This requirement allows an RSU to determine the radio coverage in each of sixteen 22.5 degree sectors around the RSU. The first sector starts from North and ends at 22.5 degrees from North in an eastward direction and the distance is measured in tenths of a meter. The message type is identified by the DE_DSRC_MessageID data element, as defined in SAE J2735_201603. The vehicle type is defined by DE_VehicleType, as defined in SAE J2735_201603, which represents the FHWA 13-Vehicle Category Classification. A distance of 0 meters indicates no messages are received.

3.5.2.8.7 Report the Average RF Communications Distance - 15 Minutes

Upon request from a management station, the RSU shall report the average farthest distance from the location of the RSU by sector from which a message was received via the V2X interface over the previous 15 minutes by message type and vehicle type. This requirement assumes that the RSU has the ability to determine when a mobile device is first or last detected by the RSU within a sector. This calculation is a simple average of the location of each mobile device detected by the RSU in the previous 15 minutes. This requirement allows an RSU to determine the radio coverage in each of sixteen 22.5 degree sectors around the RSU. The first sector starts from North and ends at 22.5 degrees from North in an eastward direction and the distance is measured in tenths of a meter. The message type is identified by the DE_DSRC_MessageID data element, as defined in SAE J2735_201603. The vehicle type is defined by DE_VehicleType, as defined in SAE J2735_201603, which represents the FHWA 13-Vehicle Category Classification. A distance of 0 meters indicates no messages are received.

3.5.2.9 Determine Application Status

Upon request by a management station, the RSU shall report the status of an application on the RSU. The status of the application is defined by if the application is active or not.

3.5.2.10 Retrieve Configuration Parameters Requirements

Requirements for retrieving the configuration parameters for the RSU follow.

3.5.2.10.1 Report the Internal Operating Temperature

Upon request from a management station, the RSU shall report the internal temperature of the RSU enclosure in degrees Celsius. The valid values are from -100 to 100 degrees Celsius, and an additional value indicating unknown temperature.

3.5.2.10.2 Determine the Internal Operating Temperature Thresholds

Upon request from a management station, the RSU shall report the internal temperature thresholds for the RSU enclosure in degrees Celsius. The valid values are from -100 to 100 degrees Celsius, and an additional value indicating unknown temperature. The RSU is to transmit a notification if the internal temperature exceeds the temperature thresholds.

3.5.2.11 Report RSU Current Status Requirements

The requirements to report the current status of the RSU follow.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

3.5.2.11.1 Report RSU Current Overall Status

Upon request from a management station, the RSU shall report the overall summary current state of the RSU. Valid values are okay, warning, critical and unknown. Okay indicates the RSU fully operational with no errors detected that impacts its operation, i.e., all services provided by the RSU are okay. Warning indicates the RSU is operating, but an issue is detected which may affect its operation, e.g., wrong configuration, firewall not active. Critical indicates an error that has a significant impact on the RSU operation, e.g., time source lost or a service crashed.

3.5.2.11.2 Report RSU Services Status Requirements

The requirements to retrieve the status of services provided by the RSU follow.

3.5.2.11.2.1 Report RSU System Services Status

Upon request from a management station, the RSU shall report the current state of the system services on the RSU. System services include CPU usage and memory usage. Valid values are okay, warning, critical and unknown. Okay indicates the system services is fully operational with no errors detected that impacts its operation. Warning indicates the system services is operational, but an error is detected which may affect its operation, e.g., low system memory available. Critical indicates an error is detected that has a significant impact on the RSU operation, e.g., no system memory available.

3.5.2.11.2.2 Report GNSS Service Status

Upon request from a management station, the RSU shall report the current state of the GNSS service on the RSU. Valid values are okay, warning, critical and unknown. Okay indicates the GNSS service is fully functional with no errors detected. Warning indicates the GNSS service is operational, but an issue is detected which may affect its operation, e.g., poor signal strength, signal from less than 5 satellites available. Critical indicates an error is detected that has a significant impact on the RSU operation, e.g., no GNSS signal detected.

3.5.2.11.2.3 Report Time Service Status

Upon request from a management station, the RSU shall report the current state of the time source on the RSU. Valid values are okay, warning, critical and unknown. Okay indicates the RSU's primary time source is fully operational with no errors detected. Warning indicates that an issue with the time source is detected, which may affect RSU operations, e.g., non-primary time source not detected, no valid time data from the primary time source but secondary time source is available, or tolerable deviation between two or more different time sources detected. Critical indicates an error is detected that has a significant impact on the RSU operation, e.g., primary clock source timeout and no other time source available.

3.5.2.11.2.4 Report Storage Service Status

Upon request from a management station, the RSU shall report the current state of the storage available for storing logs on the RSU. Valid values are okay, warning, critical and unknown. Okay indicates that sufficient storage is available for storing new log data, including removable storage (e.g., SD card). Warning indicates the available storage may be insufficient based on the current calculated storage needs. The Warning threshold may be vendor-defined or agency-defined but should be based on what the expected storage needs when considering what logging is currently enabled or scheduled. Critical indicates that no storage is available for saving logged data on the RSU (even if the RSU is writing over older log files).

3.5.2.11.2.5 Report Access Control Service Status

Upon request from a management station, the RSU shall report the current state of the access control (e.g., firewall) service on the RSU. Valid values are okay, warning, critical and unknown. Okay indicates

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

the access control service is fully operational with no errors detected. Warning indicates the access control service is operating, but an issue is detected which may compromise security, e.g., a potentially unauthorized request is detected. Critical indicates an error is detected that may comprise RSU security, e.g., the access control service has timed out.

3.5.2.11.2.6 Report Network Service Status

Upon request from a management station, the RSU shall report the current state of the network services on the RSU. Valid values are okay, warning, critical and unknown. Okay indicates the network services are fully operational with no errors detected. Warning indicates that an issue is detected with a network issues which may affect RSU operations, e.g., communications timeout. Critical indicates an error is detected that has a significant impact on the RSU operation, e.g., communications timeout with a management station.

3.5.2.11.2.7 Report Radio Access Service Status

Upon request from a management station, the RSU shall report the current state of the radio access services, such as layers 1 and 2 of the radio access technology, on the RSU. Valid values are okay, warning, critical and unknown. Okay indicates the radio services are fully operational with no errors detected. Warning indicates the radio access services are operating, but an issue is detected which may affect its operation. Critical indicates an error that has a significant impact on the RSU operation, e.g., the RSU has insufficient precision timing to perform alternating radio mode or no response from the V2X radio.

3.5.2.11.2.8 Report V2X Radio Networking Services Status

Upon request from a management station, the RSU shall report the current state of the V2X radio networking services, such as layers 3 and 4 of the radio access technology on the RSU. For DSRC radios, this represents IEEE 1609.3-2016. Valid values are okay, warning, critical and unknown. Okay indicates the radio networking services are fully operational with no errors detected. Warning indicates the radio networking services are operating, but an issue is detected which may affect its operation, e.g., wrong configuration. Critical indicates an error that has a significant impact on the RSU operation, e.g., the Ethernet interface is down or the DNS is unavailable.

3.5.2.11.2.9 Report IEEE 1609.2 Status

Upon request from a management station, the RSU shall report the current state of IEEE 1609.2 certificates on the RSU. Valid values are okay, warning, critical and unknown. Okay indicates the status of the IEEE 1609.2 certificates is fully operational with no errors detected. Warning indicates the services that use IEEE 1609.2 certificates are operational, but an issue is detected which may affect its operation, e.g., the number of valid IEEE 1609.2 certificates are low, or there is an IEEE 1609.2 application certificate expiring within 7 days. Critical indicates an error that has a significant impact on the RSU operation, e.g., no more valid IEEE 1609.2 certificates are available.

3.5.2.11.2.10 Report SCMS Service Status

Upon request from a management station, the RSU shall report the current state of the SCMS service on the RSU. Valid values are okay, warning, critical and unknown. Okay indicates the SCMS service is fully operational with no errors detected. Warning indicates the SCMS service is operating, but an issue is detected which may affect its operation, e.g., the enrollment certificates are expiring within 7 days. Critical indicates an error is detected that has a significant impact on the RSU operation, e.g., the enrollment certificates are invalid.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

3.5.2.11.2.11 Report Vendor Specific Services Status

Upon request from a management station, the RSU shall report the current state of vendor specific services on the RSU. Valid values are okay, warning, critical and unknown. Okay indicates the vendor specific service is operating properly with no errors detected and that impacts its operation. Warning indicates the vendor specific service is operating, but an issue is detected which may affect its operation. Critical indicates the vendor specific service may not be operating or an error is detected that has a significant impact on the RSU operation.

3.5.2.11.2.12 Report RSU Services Description

Upon request from a management station, the RSU shall report a detailed description of the cause of the current status of an RSU service. For example, the description may describe what event caused an RSU service to have a current state of Critical.

3.5.2.11.2.13 Report RSU Services Status Update Time

Upon request from a management station, the RSU shall report the date and time the current state of a RSU was last updated. This requirement allows a transportation operator to determine when an event that caused the service to enter a Warning or Critical state occurred.

3.5.3 RSU Control Requirements

The requirements for controlling the RSU device follow.

3.5.3.1 Control Mode of Operation

Upon request from a management station, the RSU shall change its mode of operation as requested. Valid modes of operation are fully operational, and standby mode.

3.5.3.2 Control RF Antenna Output

Upon request from a management station, the RSU shall set the transmit power of a RF channel as effective isotropic radiated power (EIRP), in dBm. The transmit power is required to comply with the appropriate regulatory domain.

3.5.3.3 Reboot RSU

Upon request from a management station, the RSU shall (warm) reboot the RSU.

3.5.3.4 Control Application

Upon request from a management station, the RSU shall enable or disable an application (process) on the RSU.

3.5.4 Security Requirements

The requirements to configure and monitor security for the RSU follows.

3.5.4.1 Configure Security Requirements

The requirements to configure and monitor security for the RSU follows.

3.5.4.1.1 Configure Authentication Requirements

The requirements to configure authentication for the RSU follows.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

3.5.4.1.1.1 Report Valid Geographic Region - Enrollment Certificates

Upon request from a management station, the RSU shall report the valid geographic region for enrollment certificates. Enrollment certificates may define a geographic region within which the certificate is valid. This requirement allows the RSU to report the valid geographic region, which is within the radius of the RSU's location in meters, so the RSU may request, receive and store an enrollment certificate with the appropriate geographic region.

3.5.4.2 Monitor Availability Requirements

The requirements to monitor for availability failures for the RSU follows.

3.5.4.2.1 Report Expiration Date - Enrollment Certificates

Upon request from a management station, the RSU shall report the number of days before the existing enrollment certificate on the RSU expire. This requirement indicates if the RSU needs to request a new enrollment certificate. A value of 0 indicates the certificates expire that day, but have not expired yet. A value of 65535 indicates the certificates have expired. A value of 65534 indicates the expiration dates are 65534 days or longer.

3.5.4.2.2 Report Expiration Date - Application Certificates

Upon request from a management station, the RSU shall report the number of hours before the existing application certificates on the RSU expire. This requirement indicates if the RSU needs to request new application certificates. A value of 0 indicates the certificates expire that day, but have not expired yet. A value of 255 indicates the certificates have expired. A value of 254 indicates the expiration dates are 254 hours or longer.

3.6 Supplemental Non-communications Requirements

Supplemental non-communications requirements for RSU follow. These requirements do not directly involve communications via the communications interfaces addressed by NTCIP 1218 v01, but, if the supplemental requirement is selected in the PRL, the implementation shall fulfill the stated requirement to claim conformance to NTCIP 1218 v01.

3.6.1 Security Requirements

Many of the security requirements (and design) for NTCIP 1218 v01 make extensive use of the SNMPv3 security mechanisms available. This decision was made because SNMPv3 provides the most straightforward path for adoption at this time but other security mechanisms exist that may also be suitable and could be defined in future updates. For example, although NTCIP 1218 v01 specifies the use of USM and TSM below, this does not preclude the use of other security mechanisms as long as that mechanism does not conflict with the following requirements.

3.6.1.1 Authenticate Authorized Messages Requirements

The requirements for the RSU to authenticate the authorized (signed) messages exchanged with the RSU follow.

3.6.1.1.1 Support SHA-1

The RSU shall support the use of SHA-1 hash function (SHA) used in HMAC-SHA-96.

> Note: NIST has disallowed the use of SHA-1 for digital signature generation (as provided in NIST FIPS 186-4) except where specifically allowed by NIST protocol-specific guidance.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

3.6.1.1.2 Support SHA-2

The RSU shall support the use of SHA-2 hash function (SHA) authentication protocol. The PRL in Table 6 specifies which authentication protocol to use.

3.6.1.2 Confidentiality Requirements

The requirements for the RSU to maintain the confidentiality of the data exchanged with the RSU follow.

3.6.1.2.1 Access RSU - USM

The RSU shall support the use of the User-based Security Model (USM) for SNMPv3 in accordance with RFC 3414.

3.6.1.2.2 Access RSU - TSM

The RSU shall support the use of the Transport Security Model (TSM) for SNMPv3 in accordance with RFC 5591, implementing DTLS (RFC 6353) at a minimum.

3.6.1.2.3 Support AES-256 Encryption

The RSU shall support the use of Advanced Encryption Standard 256-bit (AES-256) keys for encryption.

3.6.1.2.4 Support DTLS

The RSU shall support the use of the Datagram Transportation Layer Security (DTLS) Protocol as a transport model following RFC 6353.

3.6.2 Response Time for Requests

The RSU shall process all requests in accordance with all of the rules of the referenced standards (e.g., RFC 3411), including decrypting and uncompressing the request; processing certificates, updating the value in the database; and encrypting, compressing, and initiating the transmission of the appropriate response (assuming that the RSU has permission to transmit) within the Response Time. If the specification does not indicate the Response Time, the Response Time shall be less than 1000 milliseconds. The Response Time is measured as the time between the receiving of the last byte of the request and the transmission of the first byte of the response.

This is a high-level requirement. The response time requirement for a specific request is defined by the requirement the request addresses and is implementation-specific, depending on how the implementation addresses security, for example.

> Note: The original user need for this requirement for other NTCIP devices was based on systems using serial communications. For guidance, NTCIP 1103 v03 (Section 4.2.2.2) indicates the maximum response time shall be 100 milliseconds plus one millisecond for each byte in the response variable-bindings field. For testing purposes, the request consists of a single OID whose value is retrieved, e.g., rsuID.

3.6.3 Event Log Data Requirements

Supplemental requirements for logging events on the RSU follow.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

3.6.3.1 Event Log - System Events

When a system event occurs, the RSU shall write an entry in its event log containing system messages, including errors, information messages and warnings containing the following data:

a) Date and Time (in UTC) of the event
b) A description of the system event that occurred

For example, a startup of an application or when the RSU changes its operating mode should be logged as an event.

3.6.3.2 Event Log - Application Events

When an application event occurs, the RSU shall write an entry in its event log containing application messages, including errors, when application configuration change, information messages and warnings containing the following data:

a) Date and Time (in UTC) of the event
b) A description of the system event that occurred

For example, configuration of a detector zone should be logged as an event.

3.6.3.3 Event Log - RSU Configuration

When there is a change to the RSU configuration, the RSU shall write an entry in its event log containing the following data:

a) Date and Time (in UTC) of the event
b) the name and Object Identifier (OID) of the configuration parameter changed and the new value
c) User ID and the network address of the user requesting the change

3.6.3.4 Event Log - Notification

When a notification is generated by the RSU (see Section 3.5.1.1.7), the RSU shall write an entry in its event log with the notification that is transmitted to a destination network address and port number. Each entry contains the following data:

a) Date and Time (in UTC) of the notification
b) The notification message
c) The notification alert level

3.6.3.5 Event Log - Security

When an event occurs that may pose a potential security risk, such as an authentication failure, data integrity failure, availability failures (for authorized/unauthorized users), and confidentiality failures, the RSU shall write an entry in its event log. Each entry contains the following data:

a) Date and Time of the event
b) Description of the potential risk
c) User ID of the user (if applicable)
d) Network address and port of the source

3.6.3.6 Event Log - Stored Message

When an event to change a stored message on the RSU occurs, the RSU shall write an entry in its event log. The log entry contains the following data:

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

a) Date and Time (in UTC) of the event
b) The message, as stored on the RSU and identified by its index
c) Classification of the operation (installation, removal, or modification)
d) User ID of the user performing the operation

3.6.3.7 Event Log - Immediate Forward Message

When an event changing a message received for forwarding to the V2X interface occurs, the RSU shall write an entry in its event log. The intent is to log only when the table containing the IFM messages is changed, not when the contents of the message changes. The log entry contains the following data:

a) Date and Time (in UTC) of the event
b) The message received for forwarding to the V2X interface
c) Classification of the operation (installation, removal, or modification)
d) User ID of the user performing the operation

3.6.4 Interface Data Log Data Requirements

Requirements for the interface data logging services on the RSU follow.

3.6.4.1 Interface Data Log Format

Upon request from a management station, the RSU shall log interface data packets across a specified interface in the packet capture (pcap) format.

3.6.4.2 Interface Data Log File Format

Upon request from a management station, the interface data log file for the RSU shall contain the following data:

a) Date and Time, with minimum deci-seconds resolution, when the packet was logged, in UTC
b) Received Signal Strength Indication (RSSI) for packets received over the V2X interface (in units of dbm)
c) Transmit Power for packets transmitted over the V2X interface (in units of dBm)
d) Complete packet transmitted or received (including headers and footers)

3.6.4.3 Interface Data Log File Naming Convention Requirements

The requirements for the naming convention of an interface data log file for a RSU follows.

3.6.4.3.1 Support RSU Identifier in the Interface Data Log Filename

The RSU shall log interface data packets in a file using a filename consisting of the identifier of the RSU. This is the <identifier> field as defined in Section 5.8.2.8, rsuIfaceLogName.

3.6.4.3.2 Support Interface Identifier in the Interface Data Log Filename

The RSU shall log interface data packets in a file using a filename consisting of identifier of the interface. This is the <interface> field as defined in Section 5.8.2.8, rsuIfaceLogName.

3.6.4.3.3 Support Direction in the Interface Data Log Filename

The RSU shall log interface data packets in a file using a filename consisting of the direction of the communications being logged. This is the <direction> field as defined in Section 5.8.2.8, rsuIfaceLogName.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

3.6.4.3.4 Support Date and Time in the Interface Data Log Filename

The RSU shall log interface data packets in a file using a filename consisting of the date and time when the log file was created. This is the <time> field as defined in 5.8.2.8, rsuIfaceLogName.

3.6.4.4 Interface Data Logging - Operational State

The RSU shall log interface data only when the RSU is in an 'Operate' mode of operation. If the RSU transitions to another mode of operation, the RSU shall close all active (i.e., active logging) interface log files.

> Note: if this requirement is not selected, when enabled, the RSU shall log interface data regardless of the RSU's mode of operation.

3.6.4.5 Open a New Interface Data Log

The RSU shall open a new interface data log file when a previously active interface data log reaches its maximum interface data log file.

3.6.5 Copy Files using SCP

The RSU shall use Secure Copy Protocol (SCP), to copy files, such as installation files, between the RSU and a server.

3.6.6 User Accounts

The RSU shall support a minimum of two (2) user accounts, one account with full read and write access and the second account with full read access.

3.6.7 Time Fix - Alternating Mode

The RSU shall have a sufficient time fix to permit a V2X radio to operate in alternating mode.

3.6.8 Determine Maximum Number of Application Certificates Supported

The RSU shall contain sufficient storage space to store the Maximum Number of Application Certificates. To calculate the Maximum Number of Application Certificates needed, the deployer should consider the number of applications the RSU is expected to support, and the number of PSIDs that can be associated with an application certificate.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

Section 4
Dialogs [Normative]

Section 4 defines the dialogs (i.e., sequence of data exchanges) that fulfill various Data Exchange requirements defined in Section 3.5. As SNMP communications are largely driven by the management station, most of the requirements define how the device shall respond to the various possible actions a management station might take.

The NTCIP standards effort is based on SNMP. This protocol offers a high degree of flexibility as to how the management station structures its requests. For example, with SNMP, the management station can do any of the following:

a) Transmit (send) only those requests that are critical at the current time, whereas a standardized dialog typically transmits requests relating to all associated data, regardless of whether it is critical for current purposes
b) Combine a number of requests in a single packet, whereas a standardized dialog dictates the exact contents of each packet
c) Separate a group of requests into multiple packets, whereas a standardized dialog dictates the exact contents of each packet
d) Interweave requests from multiple dialogs, whereas a standardized dialog dictates the exact ordering of messages, which are not interrupted with other messages

This flexibility can be a powerful tool allowing a management system to optimize the use of communication facilities, which is the primary reason that SNMP was chosen as the core NTCIP protocol. However, the flexibility also means that there are numerous allowable variations in the management process that a management station may choose to use and that an agent shall support to conform to NTCIP 1218 v01.

Unfortunately, this flexibility presents a challenge to ensuring interoperability. While a conformant RSU is required to support all mandatory operations defined within NTCIP 1218 v01, ensuring that a given RSU actually supports every possible combination of mandatory and optional requirements would be impractical. Instead, most agencies only require that the device be tested to a standard set of procedures, which would use standardized dialogs (as defined in Section 4.2, and Annex G). To improve communications efficiency, management stations may use non-standard dialogs (e.g., a combination of GET and/or SET requests that is not defined as a standardized dialog, but which a conformant device is required to support according to the MAX-ACCESS rules defined in Section 5). Because these more efficient dialogs may not be known until the acquisition of the management station, which may be years after the acquisition of the device, there is a potential for an interoperability problem to arise.

To overcome this complication, Section 4 defines a lowest common denominator approach to communications between a management station and a device. It defines the standardized dialog for each Data Exchange Requirement. Management stations may support other dialogs to fulfill these same requirements, as long as these dialogs are consistent with the rules defined in NTCIP 1218 v01. Such a management station is termed a “consistent management station.” A consistent management station interoperates with any “conformant” device. However, since an agency cannot be certain that a device is 100% conformant to every possible scenario (given practical constraints), interoperability problems could still arise.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

A “conformant management station” is required to offer a mode in which it only uses the standardized dialogs as defined in Section 4. With this limited definition, there is relatively little variability in what constitutes a conformant management station. Thus, fully testing a management station for conformance is a relatively straight forward process that can be done within the practical constraints faced by most procuring agencies. Thus, a conformant management station provides an agency with a much greater chance of achieving interoperability with off-the-shelf devices that have been tested against NTCIP 2104 v03, and the designation of such a system is intended to provide a guaranteed base level of interoperability.

The rules for the standardized dialogs follow:

a) The dialogs are defined by a sequence of GET or SET requests. These requests shall equate to the GET and SET operations defined in Annexes G.1 and G.3 and shall be transmitted as a single message.
b) The contents of each request are identified by an object name. Each object name consists of an object type and an instance identifier. Definitions of each object type are provided in Section 5 and NTCIP 1201 v03. The meaning of the instance identifier is provided by these same definitions coupled with standard SNMP rules (see RFC 2578).
c) Each message shall contain all of the objects as shown, unless otherwise indicated
d) A message shall not contain any other objects
e) The contents of each message sent by the management station may appear in any order

   Note: Ideally, the order of objects should match the order as shown in NTCIP 1218 v01 to provide the highest probability of interoperability. However, it is recognized that many implementations may use off-the-shelf software, which may prevent the designation of an exact ordering of objects and as a result, this ordering is not a requirement of NTCIP 1218 v01.

f) After transmitting (sending) a message, the management station shall not transmit any other data to that device until the earlier of:

   1) The management station receiving a response from the device; or
   2) The expiration of the maximum response time.

g) If the response indicates an error occurred in the operation, the management station shall exit the process, unless specific error-handling rules are specified by the dialog.
h) Dialogs containing a sequence of only GET requests may request objects in any order.

However, since consistent management stations can alter the order of requests, NTCIP 1218 v01 defines rules for when certain data exchanges are allowed. Unless otherwise indicated, a conformant device shall allow an object to be retrieved (through a GET request) or altered (through a SET request, if the object is writable) at any time.

Finally, Section 4 presents an overview of all of the data defined by NTCIP 1218 v01, prior to presenting the complete definition for each piece of data in Section 5.

4.1 Tutorial [Informative]

The Requirements Traceability Matrix (RTM) in Annex A.3 identifies the standardized dialog that can be used to achieve each of the data exchange requirements defined in Section 3.5. Simple data exchange requirements reference one of the generic SNMP dialogs along with a list of data elements (See Annex G). These equate to a single message being sent (e.g., a GET request) containing the referenced data elements followed by the appropriate response per the generic dialog specification.

Section 4.2 and Annex G define the standardized dialogs for the more complicated data exchange requirements. Each dialog in these sections define how the system is designed to work for a given data exchange requirement. It indicates the sequence of actions that a management station has to follow to

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

provide the specific service. Each of these dialogs is defined by a number of steps. Many of the steps reference data elements that are defined in Section 5 or in NTCIP 1201 v03. These data elements are also shown in the corresponding row of the RTM along with their precise section number.

The dialogs may also be accompanied by an informative figure that provides a graphical depiction of the normative text. The figures conform to the Unified Modeling Language and depict the management station as an outside actor transmitting (sending) a series of messages to the device and the device returning responses. If there is any conflict between the figure and the text, the text takes precedence.

4.2 Specified Dialogs

This section provides the standardized data exchange sequences that can be used by management stations to ensure interoperable implementations for the various data exchange requirements identified in Section 3. Diagrams and graphical representations are included to supplement the text (i.e., not used as a replacement for the text). This section only includes dialogs that have special semantics or impose special restrictions on the operations that are allowed.

4.2.1 Generic Retrieve Table Dialog - Static Table

Note: This is a generic dialog that is referenced by requirements in the RTM with specific object names in a static table. This generic dialog does NOT supersede the requirements and mechanism of the Block Object management defined in NTCIP 1201 v03, Section 2.3 and Annex A.1.

The list of objects provided by the specific dialog shall include:

a) an object that indicates the number of rows in the table,
b) the object(s) that serve as the index field of the table row, and
c) the list of columnar objects to be retrieved from the table.

The standardized dialog for a management station to retrieve a table shall be as follows:

a) The management station shall GET the number of rows in the table.
b) For each row of the table, the management station shall GET all objects referenced by the specific dialog that references this generic dialog, except for the number of rows object and the index object(s).

For example, the standardized dialog for a management station to identify the hardware and software configuration of a NTCIP device would be as follows:

a) The management station shall GET the object globalMaxModules.0.
b) For each row in the module table, the management station shall GET the following objects:

    1) moduleDeviceNode.x,
    2) moduleMake.x,
    3) moduleModel.x,
    4) moduleVersion.x,
    5) moduleType.x.

Where:

x = module number

4.2.2 Generic Retrieve Table Row Dialog

Note: This is a generic dialog that is referenced by other dialogs with specific object names.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

The list of objects provided by the specific dialog shall include:

a) the object(s) that serve as the index field of the table row, and
b) the list of columnar objects to be retrieved from the table.

The standardized dialog for a management station to retrieve a table shall be as follows:

a) (Precondition) The management station shall be aware of which row of the table is to be retrieved.
b) For the specified row, the management station shall GET all objects referenced by the specific dialog that references this generic dialog, except for the index object(s).

4.2.3 Generic Configure Table Row Dialog

Note: This is a generic dialog that is referenced by other dialogs with specific object names. The list of objects provided by the specific dialog shall include:

a) the object(s) that serve as the index field of the table row, and
b) the list of columnar objects to be configured and their desired values.

The standardized dialog for a management station to configure a table row shall be as follows:

a) (Precondition) The management station shall be aware of which row in the table is to be configured.
b) For the specified row, the management station shall SET all objects (to their desired values) referenced by the specific dialog that references this generic dialog, except for the index object(s).

4.2.4 Generic Retrieve Table Dialog - Dynamic Table

Note: This is a generic dialog that is referenced by requirements in the RTM with specific object names in a dynamic table. This generic dialog does NOT supersede the requirements and mechanism of the Block Object management defined in NTCIP 1201 v03, Section 2.3 and Annex A.1.

The list of objects provided by the specific dialog shall include:

a) the object(s) that serve as the index field of the table row, and
b) the list of columnar objects to be retrieved from the table.

The standardized dialog for a management station to retrieve a table shall be as follows:

a) For each row of the table, the management station shall GET all objects referenced by the specific dialog that references this generic dialog, except for the index object(s).

4.2.5 Secure Copy Protocol Dialog

Note: This is a generic dialog that is referenced by requirements in the RTM with a specific object name that either contains the name of a file to be copied, or contains the directory with the files to be copied.

The device shall adhere to the following rules:

a) If the object points to a directory path, that directory path is the base directory and a user cannot traverse to any parent directory.
b) If the object points to a directory path, subdirectories that are not links may be used.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

4.2.6 Secure Installation Dialog

This dialog is used to install firmware updates, applications, or component updates on the RSU. This dialog allows an agency to copy an installation file to the RSU, identify the location and name of the installation file, start a process to install the necessary components on the RSU, then confirm that the installation was properly completed. The installation file for the RSU is analogous to an installation file in Microsoft Windows. NTCIP 1218 v01 does not identify the format of the installation file nor does it define how the installation process works. The installation process also should consider the authentication and integrity of the installation file, and any encryption that may be used in compliance with the appropriate agency policies.

The standardized dialog for a management station to install new software components on the RSU shall be as follows:

a) (Preconditions) The software installation package shall contain all the necessary components to be installed.
b) (Preconditions) The management station shall be aware of the filename of the source file containing the package to be installed on the RSU.
c) The management station shall GET rsuInstallPath to identify the target directory of where the installation file is copied to.
d) The management station shall SET rsuInstallFile to identify the target filename of the package to be installed on the RSU.
e) The management station copy the source file to the target directory and filename using 4.2.5 Secure Copy Protocol Dialog.
f) The management station shall SET rsuInstallUpdate to 'TRUE" to begin the installation.
g) The management station shall GET rsuInstallStatus.
h) If the response is 'processing' the RSU is processing the installation of the package. The management station shall continue to GET rsuInstallStatus until the response is any other value than 'processing'.
i) If the response is 'rejected' or 'rollback', the RSU has encountered an error and the management station shall exit this process and determine the source of the error.
j) No guidance is provided if the response is 'other' or 'unknown'. A response of 'other' generally indicates a vendor-specific error.
k) If the response is 'successful', the installation process is complete and the management station shall either GET the rsuFirmwareVersion or GET the contents of the globalModuleTable to confirm the module and firmware version information has been properly updated. The RSU shall then exit this process.

4.2.7 Retrieve Event Logged Data Dialog

This dialog allows a transportation operator to generate and download a copy of the logged event data in the RSU's system log (syslog) file. NTCIP 1218 v01 allows the transportation operator to filter the logged event data in the copy of the syslog file by (start and stop) time and severity.

The standardized dialog for a management station to retrieve logged data from the RSU's system log shall be as follows:

a) The management station shall SET rsuSysLogQueryGenerate to '1'.
b) The RSU shall create a copy of the syslog file using the values in rsuSysLogQueryStart, rsuSysLogQueryStop, and rsuSysLogQueryPriority to filter the events.
c) The management station shall GET rsuSysLogQueryStatus.
d) If the response is 'processing' the RSU is processing the logged event data. The management station shall continue to GET rsuSysLogQueryStatus until the response is any other value than 'processing'.
e) If the response is 'outOfRange' or 'badFilename', the RSU has encountered an error and the

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

management station shall exit this process and determine the source of the error.

f) No guidance is provided if the response is 'other' or 'unknown'. A response of 'other' generally indicates a vendor-specific error.
g) If the response is 'successful', the installation process is complete and the management station shall download the copy of the syslog file from the RSU using the Secure Copy Protocol Dialog (See Section 4.2.5). The value of the rsuSysLogName contains the directory and filename of the copy of the syslog file, relative to the base directory, which is provided by rsuSysDir. The management station shall then exit this process.

4.3 State-Transition Diagrams

State-Transition diagrams are included for those objects that have states or manage states. The State Transition Diagrams include state-transition tables (listing of the possible state transitions), legitimate transitions, and any illegitimate transitions.

"State-transition diagrams describe all of the states that an object can have, the events under which an object changes state (transitions), the conditions that must be fulfilled before the transition will occur (guards), and the activities undertaken during the life of an object (actions)." (See *State-Transition Diagrams: Testing UML Models, Part 4,* Copeland, Lee)

Definitions of the states for various object classes that may be supported by the RSU follow.

4.3.1 Operating Mode State Machine Definition

The RSU shall allow a management station to manage the mode of operation of the RSU.

4.3.1.1 Operating Mode

When in the 'operating' mode, the following rules shall apply to the RSU:

a) If rsuMode is SET to 'standby', the RSU shall transfer to the Standby mode.
b) Any V2X radio may be enabled (to transmit or receive).
c) Interface logging may be enabled.

4.3.1.2 Standby Mode

When in the 'standby' mode, the following rules shall apply to the RSU:

a) If rsuMode is SET to 'operate', the RSU shall transfer to the Operating mode.
b) All V2X radios are not enabled (to transmit or receive).
c) All interface logging is disabled.
d) The RSU shall return a 'genErr' error for any SET to enable a V2X radio.
e) The RSU shall return a 'genErr' error for any SET to enable interface logging.

4.3.1.3 Fault Mode

When in the 'fault' mode, the following rules shall apply to the RSU:

a) If RSU shall return a 'genErr' error for any SET request from a management station.
b) All V2X radios are not enabled (to transmit or receive).
c) All interface logging is disabled.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

Section 5
Management Information Base (MIB) [Normative]

Section 5 defines those objects that are specifically used by RSUs). The objects are defined using the OBJECT-TYPE macro as specified in RFCs 2578, 2579, and 2580. The text provided in Section 5 (except the section headings) constitutes the standard NTCIP1218-v01 MIB.

All of the objects defined in this NTCIP 1218 v01 reside under the “rsu” node of the global naming tree. To aid in object management, the “rsu” node has been subdivided into logical categories, each defined by a node under the “rsu” node. The individual objects are then located under the appropriate node.

Conformance requirements for any object are determined by the use of the Requirements Traceability Matrix (RTM) in Annex A. To support any defined Requirement, an implementation shall support all objects to which the Requirement traces in the RTM. The value of the STATUS field for every object in the MIB is "mandatory," and indicates that it is mandatory if any associated Requirement is selected.

For all bitmapped objects, if a bit is zero (0), then the referenced function is disabled or not supported, and if a bit is one (1), then the referenced function is enabled or supported.

A computer readable format of this information, called a Management Information Base, is available from NEMA (ntcip@nema.org). The MIB has been verified using Unbrowse SNMP version 1.6.0.1342 (https://www.unleashnetworks.com/products/unbrowse-snmp.html) and SMI SNMP Validator based on libsmi (smilint 0.4.7) (https://www.simpleweb.org/ietf/mibs/validate/).

5.0 MIB Comment Header

```
--*****************************************************************
-- Filename:      1218v0138.MIB
-- Date:          September 4, 2020
-- Description:   This MIB defines the Roadside Unit (RSU) Objects
--*****************************************************************
```

5.1 MIB Header

```
NTCIP1218-v01 DEFINITIONS ::= BEGIN

-- the following OBJECT IDENTIFIERS are used in the RSU MIB:
IMPORTS
      MODULE-IDENTITY, OBJECT-TYPE, Integer32, Counter32, NOTIFICATION-TYPE,
      enterprises
                  FROM SNMPv2-SMI
      TEXTUAL-CONVENTION, DateAndTime, RowStatus, DisplayString, MacAddress
            FROM SNMPv2-TC
      SyslogSeverity
            FROM SYSLOG-TC-MIB
      Uri255, Uri1024
            FROM URI-TC-MIB;

rsu MODULE-IDENTITY
      LAST-UPDATED      "202009040000Z"
      ORGANIZATION      "NTCIP - AASHTO/ITE/NEMA"
      CONTACT-INFO      "postal:    NTCIP Coordinator
```

© 2020 AASHTO / ITE / NEMA

```
                        National Electrical Manufacturers Association
                        1300 North 17th Street, Suite 900
                        Rosslyn, Virginia  22209-3801
                        email:           ntcip@nema.org"
      DESCRIPTION       "This MIB defines the Roadside Unit (RSU) Objects"
      REVISION          "202009040000Z"
      DESCRIPTION       "Published Version"
      ::= { devices 18 }

-- A.2 STRUCTURE INFORMATION
nema                    OBJECT IDENTIFIER  ::=  { enterprises 1206 }
-- NEMA has received ID 1206 from IANA
-- NEMA starts at { iso org dod internet private enterprises 1206 } in the
-- global naming tree.

transportation          OBJECT IDENTIFIER  ::=  { nema 4 }
-- The transportation subtree is used by the NTCIP to define
-- standard objects specific for the transportation industry.

devices           OBJECT IDENTIFIER  ::=  { transportation 2 }
Also
RsuTableIndex ::= TEXTUAL-CONVENTION
    DISPLAY-HINT   "d"
    STATUS         current
    DESCRIPTION    "A valid range of values for use in table indices"
    SYNTAX         Integer32 (1..2147483647)

RsuPsidTC ::= TEXTUAL-CONVENTION
    DISPLAY-HINT   "4x"
    STATUS         current
    DESCRIPTION    "PSID associated with a SAE J2735 message. The PSID is
         formatted per IEEE1609.12-2016 Table 2 as P-encoded hex values, e.g.
         BSM = 0x20, TIM = 0x8003, WSA = 0x8007, IProuting = 0xEFFFFFFE. For
         those PSIDs less than 4 octets in length, the RSU should only
         require the significant octets be provided. For example, if the
         desired PSID is 0x20, then the RSU should accept a supplied value of
         0x20. should not need to be padded to a 4-octet length."
    SYNTAX         OCTET STRING (SIZE(1..4))

-- For NTCIP 1218.
-- DateAndTime ::= TEXTUAL-CONVENTION
--    DISPLAY-HINT "2d-1d-1d,1d:1d:1d.1d"
--    STATUS       current
--    DESCRIPTION  "A date-time specification."
--    SYNTAX       OCTET STRING (SIZE(8))
```

5.2 RSU Radios

```
rsuRadio OBJECT IDENTIFIER ::= { rsu 1 }
```

5.2.1 Maximum Radios

```
maxRsuRadios OBJECT-TYPE
    SYNTAX       Integer32 (1..16)
    UNITS        "radio"
    MAX-ACCESS   read-only
    STATUS       current
```

 © 2020 AASHTO / ITE / NEMA

```
    DESCRIPTION  "<Definition> The maximum number of V2X radios this Roadside
         Unit supports. This object indicates the maximum rows which appears
         in the rsuRadioTable object.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.1.1"
::= { rsuRadio 1 }
```

5.2.2 Radio Table

```
rsuRadioTable OBJECT-TYPE
    SYNTAX       SEQUENCE OF RsuRadioEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> A table containing the V2X radio parameters.
         The number of rows in this table is equal to the maxRsuRadios
         object.
    <TableType> static
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.1.2"
::= { rsuRadio 2 }

rsuRadioEntry OBJECT-TYPE
    SYNTAX       RsuRadioEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Parameters for a specific roadside unit V2X
         radio.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.1.2.1"
    INDEX { rsuRadioIndex }
::= { rsuRadioTable 1 }

RsuRadioEntry ::= SEQUENCE {
    rsuRadioIndex        Integer32,
    rsuRadioDesc         DisplayString,
    rsuRadioEnable       INTEGER,
    rsuRadioType         INTEGER,
    rsuRadioMacAddress1  MacAddress,
    rsuRadioMacAddress2  MacAddress,
    rsuRadioChanMode     INTEGER,
    rsuRadioCh1          Integer32,
    rsuRadioCh2          Integer32,
    rsuRadioTxPower1     Integer32,
    rsuRadioTxPower2     Integer32 }
```

5.2.2.1 RSU Radio Index

```
rsuRadioIndex OBJECT-TYPE
    SYNTAX       Integer32 (1..16)
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Roadside unit V2X radio index.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.1.2.1.1"
::= { rsuRadioEntry 1 }
```

5.2.2.2 RSU Radio Description

```
rsuRadioDesc OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..144))
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

```
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Name of the radio that the configuration
         relates to.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.1.2.1.2"
::= { rsuRadioEntry 2 }
```

5.2.2.3 RSU Radio Enable

```
rsuRadioEnable OBJECT-TYPE
    SYNTAX       INTEGER { off(0), on(1) }
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Set this bit to 1 to enable the V2X radio for
         transmission and reception of messages, and to 0 to disable the V2X
         radio.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.1.2.1.3"
::= { rsuRadioEntry 3 }
```

5.2.2.4 RSU Radio Type

```
rsuRadioType OBJECT-TYPE
    SYNTAX       INTEGER { other(1),
                 dsrc(2),
                 pC5(3) }
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Indicates the type of V2X Radio. pC5 is
         cellular V2X.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.1.2.1.4"
::= { rsuRadioEntry 4 }
```

5.2.2.5 RSU Radio MAC Address 1

```
rsuRadioMacAddress1 OBJECT-TYPE
    SYNTAX       MacAddress
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Represents an 802 MAC address of the V2X Radio
         represented in the 'canonical' order defined by IEEE 802.1a, i.e.,
         as if it were transmitted least significant bit first, even though
         802.5 (in contrast to other 802.x protocols) requires MAC addresses
         to be transmitted most significant bit first. For a PC5 radio, use
         the least significant 24-bit for the MAC address (Layer 2 Source
         id). If the MacAddress is not available, set the MacAddress to all
         ones (1).
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.1.2.1.5"
::= { rsuRadioEntry 5 }
```

5.2.2.6 RSU Radio MAC Address 2

```
rsuRadioMacAddress2 OBJECT-TYPE
    SYNTAX       MacAddress
    MAX-ACCESS   read-only
    STATUS       current
```

 © 2020 AASHTO / ITE / NEMA

```
    DESCRIPTION  "<Definition> Represents the second IEEE 802 MAC address of
         the V2X Radio operating on a channel switch. The MAC address is as
         if the represented in the 'canonical' order defined by IEEE 802.1a,
         i.e., as if it were transmitted least significant bit first, even
         though 802.5 (in contrast to other 802.x protocols) requires MAC
         addresses to be transmitted most significant bit first. If the
         MacAddress is not available or if the radio doesn't have a second
         MAC, set the MacAddress to all ones (1).
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.1.2.1.6"
::= { rsuRadioEntry 6 }
```

5.2.2.7 RSU Radio Channel Mode

```
rsuRadioChanMode OBJECT-TYPE
    SYNTAX       INTEGER { other (1),
                 unknown (2),
                 cont (3),
                 alt (4),
                 immediate (5) }
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Represents the channel access mode for the
         radio. Supported values are continuous access (cont), alternating
         access (alt), and immediate access as defined in IEEE 1609.3-2016. A
         SET to a value of other (1) or unknown (2) shall return a badValue
         error.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.1.2.1.7"
::= { rsuRadioEntry 7 }
```

5.2.2.8 RSU Radio Channel 1

```
rsuRadioCh1 OBJECT-TYPE
    SYNTAX       Integer32 (0..255)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Represents the channel number for continuous
         mode as well as for time slot 0 when the radio is operating in
         alternating mode. For DSRC radios in the United States, the
         transmission channel is from 172 to 184, as defined by IEEE 802.11.
         For PC5 radios in the United States, the relationship between IEEE
         802.11 and 3GPP channel numbers is found in Table 7 of NTCIP 1218
         v01.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.1.2.1.8"
::= { rsuRadioEntry 8 }
```

5.2.2.9 RSU Radio Channel 2

```
rsuRadioCh2 OBJECT-TYPE
    SYNTAX       Integer32 (0..255)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Represents the channel number for channel slot
         2. For DSRC radios in the United States, the transmission channel is
         from 172 to 184, as defined by IEEE 802.11. For PC5 radios in the
         United States, the relationship between IEEE 802.11 and 3GPP channel
         numbers is found in Table 7 of NTCIP 1218 v01. If the radio operates
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

```
         in continuous mode, this value is equal to rsuRadioCh1 and is
         ignored.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.1.2.1.9"
::= { rsuRadioEntry 9 }
```

5.2.2.10 RSU Radio Channel 1 - Default Transmit Power

```
rsuRadioTxPower1 OBJECT-TYPE
    SYNTAX       Integer32 (-128..127)
    UNITS        "dBm"
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Sets the output power for channel slot 1, in
        dBm, at the V2X antenna port. This object is considered a default
        transmit power level to be used if a power level is not defined by an
        application. The power level defined by the application would take
        precedence.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.1.2.1.10"
    DEFVAL { -128 }
::= { rsuRadioEntry 10 }
```

5.2.2.11 RSU Radio Channel 2 - Default Transmit Power

```
rsuRadioTxPower2 OBJECT-TYPE
    SYNTAX       Integer32 (-128..127)
    UNITS        "dBm"
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Sets the output power for channel slot 2, in
        dBm, at the V2X antenna port. This object is considered a default
        transmit power level to be used if a power level is not defined by an
        application. The power level defined by the application would take
        precedence. If the radio operates in continuous mode, this value is
        equal to rsuRadioTxPower1 and is ignored.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.1.2.1.11"
    DEFVAL { -128 }
::= { rsuRadioEntry 11 }
```

5.3 RSU GNSS

```
rsuGnss OBJECT IDENTIFIER ::= { rsu 2 }
```

5.3.1 GNSS Status

```
rsuGnssStatus OBJECT-TYPE
    SYNTAX       Integer32 (0..128)
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Provides the number of GNSS satellites the
         RSU's internal GNSS receiver is tracking and using.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.2.1"
::= { rsuGnss 1 }
```

 © 2020 AASHTO / ITE / NEMA

5.3.2 GNSS Augmentation

```
rsuGnssAugmentation OBJECT-TYPE
    SYNTAX       INTEGER { other (1),
                 none (2),
                 waas (3) }
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "<Definition> This object indicates if the position from a
         GNSS or similar geopositioning device is augmented, such as Wide
         Area Augmentation System (WAAS) corrections.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.2.2"
    DEFVAL { none }
::= { rsuGnss 2 }
```

5.4 Store and Repeat Messages

```
rsuMsgRepeat OBJECT IDENTIFIER ::= { rsu 3 }
```

5.4.1 Maximum Number of Store and Repeat Messages

```
maxRsuMsgRepeat OBJECT-TYPE
    SYNTAX       Integer32 (1..255)
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> The maximum number of Store and Repeat
         messages this Roadside Unit supports. This object indicates the
         maximum rows which appears in the rsuMsgRepeatStatusTable object.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.3.1"
::= { rsuMsgRepeat 1 }
```

5.4.2 Store and Repeat Table

```
rsuMsgRepeatStatusTable OBJECT-TYPE
    SYNTAX       SEQUENCE OF RsuMsgRepeatStatusEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Provides configuration information for each
         Store and Repeat message to be sent by a Roadside Unit.
    <TableType>  dynamic
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.3.2"
::= { rsuMsgRepeat 2 }

rsuMsgRepeatStatusEntry OBJECT-TYPE
    SYNTAX RsuMsgRepeatStatusEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> A row describing an RSU Store and Repeat
         Message.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.3.2.1"
    INDEX      { rsuMsgRepeatIndex }
::= {rsuMsgRepeatStatusTable 1 }

RsuMsgRepeatStatusEntry ::= SEQUENCE {
    rsuMsgRepeatIndex             RsuTableIndex,
    rsuMsgRepeatPsid              RsuPsidTC,
    rsuMsgRepeatTxChannel         Integer32,
```

© 2020 AASHTO / ITE / NEMA

```
    rsuMsgRepeatTxInterval        Integer32,
    rsuMsgRepeatDeliveryStart     DateAndTime,
    rsuMsgRepeatDeliveryStop      DateAndTime,
    rsuMsgRepeatPayload           OCTET STRING,
    rsuMsgRepeatEnable            INTEGER,
    rsuMsgRepeatStatus            RowStatus,
    rsuMsgRepeatPriority          Integer32,
    rsuMsgRepeatOptions           BITS  }
```

5.4.2.1 Stored Message Index

```
rsuMsgRepeatIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Store and Repeat Message Index. This index
         shall not exceed maxRsuMsgRepeat.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.3.2.1.1"
::= { rsuMsgRepeatStatusEntry 1 }
```

5.4.2.2 Stored Message PSID

```
rsuMsgRepeatPsid OBJECT-TYPE
    SYNTAX       RsuPsidTC
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> The Provider Service Identifier (PSID) for the
         Store and Repeat Message. The current PSID assignments can be found
         at https://standards.ieee.org/products-
         services/regauth/psid/public.html.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.3.2.1.2"
::= { rsuMsgRepeatStatusEntry 2 }
```

5.4.2.3 Stored Message Transmission Channel

```
rsuMsgRepeatTxChannel OBJECT-TYPE
    SYNTAX       Integer32 (0..255)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> The transmission channel the Store and Repeat
         Message is to be transmitted. For DSRC radios in the United States,
         the transmission channel is from 172 to 184, as defined by IEEE
         802.11. For PC5 radios in the United States, the channel number is
         found in Table 7 of NTCIP 1218 v01.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.3.2.1.3"
::= { rsuMsgRepeatStatusEntry 3 }
```

5.4.2.4 Stored Message Transmission Interval

```
rsuMsgRepeatTxInterval OBJECT-TYPE
    SYNTAX       Integer32 (1..2147483647)
    UNITS        "millisecond"
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Time interval in milliseconds between the
         transmission of two successive Store and Repeat Messages.
```

 © 2020 AASHTO / ITE / NEMA

```
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.3.2.1.4"
::= { rsuMsgRepeatStatusEntry 4 }
```

5.4.2.5 Stored Message Start Time

```
rsuMsgRepeatDeliveryStart OBJECT-TYPE
    SYNTAX       DateAndTime
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Store and Repeat Message delivery start time
         in UTC. DateAndTime of length 8 octets.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.3.2.1.5"
::= { rsuMsgRepeatStatusEntry 5 }
```

5.4.2.6 Stored Message Stop Time

```
rsuMsgRepeatDeliveryStop OBJECT-TYPE
    SYNTAX       DateAndTime
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Store and Repeat Message delivery stop time in
         UTC. DateAndTime of length 8 octets.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.3.2.1.6"
::= { rsuMsgRepeatStatusEntry 6 }
```

5.4.2.7 Stored Message Payload

```
rsuMsgRepeatPayload OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(0..2302))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Payload of Store and Repeat message. Length
         limit derived from IEEE1609dot3-MIB. For SAE J2735-201603 messages,
         this object is the UPER encoded MessageFrame.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.3.2.1.7"
::= { rsuMsgRepeatStatusEntry 7 }
```

5.4.2.8 Stored Message Enabled Transmission

```
rsuMsgRepeatEnable OBJECT-TYPE
    SYNTAX       INTEGER { off (0), on (1) }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Set this bit to enable transmission of the
         message. 0=off/do not transmit, 1=on/transmit.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.3.2.1.8"
::= { rsuMsgRepeatStatusEntry 8 }
```

5.4.2.9 Stored Message Status

```
rsuMsgRepeatStatus OBJECT-TYPE
    SYNTAX       RowStatus
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Create (4) and (6) destroy row entry.
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

```
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.3.2.1.9"
::= { rsuMsgRepeatStatusEntry 9 }
```

5.4.2.10 Stored Message Priority

```
rsuMsgRepeatPriority OBJECT-TYPE
    SYNTAX       Integer32 (0..63)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Priority assigned to the Store and Repeat
         message. Priority values are defined by IEEE 1609.3-2016 for DSRC
         radios.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.3.2.1.10"
::= { rsuMsgRepeatStatusEntry 10 }
```

5.4.2.11 Stored Message Options

```
rsuMsgRepeatOptions OBJECT-TYPE
    SYNTAX       BITS { bypass(0),
                 secure(1),
                 shortTerm(2),
                 longTerm(3) }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> A bit-mapped value as defined below for
         configuring the message.
         Bit 0        0=Bypass1609.2, 1=Process1609.2
         Bit 1        0=Secure, 1=Unsecure
         Bit 2        0=ContXmit, 1=NoXmitShortTermXceeded
         Bit 3        0=ContXmit, 1=NoXmitLongTermXceeded

    Bit 0 - Indicates if the RSU is to bypass 1609.2 processing of the
         message to the V2X interface. This allows the RSU to send the
         message that has been signed and/or encrypted by the TMC. Note the
         RSU would still wrap the message payload in a WSMP header.
    Bit 1 - Indicates if the message should be secured (signed or encrypted)
         prior to transmission to the V2X Interface. How the message is to be
         secured is determined by its security profile. This bit is ignored
         if Bit 0=0 (bypass).
    Bit 2 - Indicates if the message should continue to be transmitted if the
         short-term communications loss period (rsuShortCommLossTime) is
         exceeded. 0 indicates the message should continue to be transmitted.
         Default value is 0.
    Bit 3 - Indicates if the message should continue to be transmitted if the
         long-term communications loss period (rsuLongCommLossTime) is
         exceeded. 0 indicates the message should continue to be transmitted.
         Default value is 0.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.3.2.1.11"
::= { rsuMsgRepeatStatusEntry 11 }
```

5.4.3 Delete All Stored Messages

```
rsuMsgRepeatDeleteAll OBJECT-TYPE
    SYNTAX       INTEGER (0..1)
    MAX-ACCESS   read-write
    STATUS       current
```

 © 2020 AASHTO / ITE / NEMA

```
    DESCRIPTION  "<Definition> This object when set to TRUE (one) shall cause
         the Roadside Unit to delete (destroy) all stored messages in the
         rsuMsgRepeatStatusTable. This object shall automatically return to
         FALSE (zero) after all rows in the rsuMsgRepeatStatusTable have been
         deleted.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.3.3"
::= { rsuMsgRepeat 3 }
```

5.5 Immediate Forward Messages

```
rsuIFM OBJECT IDENTIFIER ::= { rsu 4 }
```

5.5.1 Maximum Number of Immediate Forward Messages

```
maxRsuIFMs OBJECT-TYPE
    SYNTAX       Integer32 (1..255)
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> The maximum number of Immediate Forward
         messages this Roadside Unit supports. This object indicates the
         maximum rows which appears in the rsuIFMStatusTable object.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.4.1"
::= { rsuIFM 1 }
```

5.5.2 Immediate Forward Table

```
rsuIFMStatusTable OBJECT-TYPE
    SYNTAX SEQUENCE OF RsuIFMStatusEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Provides configuration parameters for each
         Immediate Forward message sent by a Roadside Unit.
    <TableType>  dynamic
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.4.2"
::= { rsuIFM 2 }

rsuIFMStatusEntry OBJECT-TYPE
    SYNTAX       RsuIFMStatusEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> A row describing an RSU Immediate Forward
         Message Status.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.4.2.1"
    INDEX   { rsuIFMIndex }
::= {rsuIFMStatusTable 1 }

RsuIFMStatusEntry ::= SEQUENCE {
    rsuIFMIndex             RsuTableIndex,
    rsuIFMPsid              RsuPsidTC,
    rsuIFMTxChannel         Integer32,
    rsuIFMEnable            INTEGER,
    rsuIFMStatus            RowStatus,
    rsuIFMPriority          Integer32,
    rsuIFMOptions           BITS,
    rsuIFMPayload           OCTET STRING }
```

© 2020 AASHTO / ITE / NEMA

5.5.2.1 Forward Message Index

```
rsuIFMIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Immediate Forward Message Index. This index
         shall not exceed maxRsuIFMs.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.4.2.1.1"
::= { rsuIFMStatusEntry 1 }
```

5.5.2.2 Forward Message PSID

```
rsuIFMPsid OBJECT-TYPE
    SYNTAX       RsuPsidTC
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> The Provider Service Identifier (PSID) for the
         Immediate Forward Message. The current PSID assignments can be found
         at https://standards.ieee.org/products-
         services/regauth/psid/public.html.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.4.2.1.2"
::= { rsuIFMStatusEntry 2}
```

5.5.2.3 Forward Message Transmission Channel

```
rsuIFMTxChannel OBJECT-TYPE
    SYNTAX       Integer32 (0..255)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> The transmission channel the Immediate Forward
         Message is to be transmitted. For DSRC radios in the United States,
         the transmission channel is from 172 to 184, as defined by IEEE
         802.11. For PC5 radios in the United States, the channel number is
         found in Table 7 of NTCIP 1218 v01.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.4.2.1.3"
::= { rsuIFMStatusEntry 3 }
```

5.5.2.4 Forward Message Enable

```
rsuIFMEnable OBJECT-TYPE
    SYNTAX       INTEGER { off (0), on (1) }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Set this bit to enable transmission of the
         message. 1 is to enable transmission.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.4.2.1.4"
::= { rsuIFMStatusEntry 4 }
```

5.5.2.5 Forward Message Status

```
rsuIFMStatus OBJECT-TYPE
    SYNTAX       RowStatus
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Create (4) and destroy (6) row entry.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.4.2.1.5"
```

Copy Per MIB Distribution Permission © 2020 AASHTO / ITE / NEMA

```
::= { rsuIFMStatusEntry 5 }
```

5.5.2.6 Forward Message Priority

```
rsuIFMPriority OBJECT-TYPE
    SYNTAX       Integer32 (0..63)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Priority assigned to the Immediate Forward
         message. Priority values defined by IEEE 1609.3-2016 for DSRC
         radios.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.4.2.1.6"
::= { rsuIFMStatusEntry 6 }
```

5.5.2.7 Forward Message Options

```
rsuIFMOptions OBJECT-TYPE
    SYNTAX       BITS { bypass(0),
                 secure(1),
                 shortTerm(2),
                 longTerm(3) }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> A bit-mapped value as defined below for
         configuring the message.
         Bit 0        0=Bypass1609.2, 1=Process1609.2
         Bit 1        0=Secure, 1=Unsecure
         Bit 2        0=ContXmit, 1=NoXmitShortTermXceeded
         Bit 3        0=ContXmit, 1=NoXmitLongTermXceeded

    Bit 0 - Indicates if the RSU is to bypass 1609.2 processing of the
         message to the V2X interface. This allows the RSU to send the
         message that has been signed and/or encrypted by the TMC. Note the
         RSU would still wrap the message payload in a WSMP header.
    Bit 1 - Indicates if the message should be secured (signed or encrypted)
         prior to transmission to the V2X Interface. How the message is to be
         secured is determined by its security profile. This bit is ignored
         if Bit 0=0 (bypass).
    Bit 2 - Indicates if the message should continue to be transmitted if the
         short-term communications loss period (rsuShortCommLossTime) is
         exceeded. 0 indicates the message should continue to be transmitted.
         Default value is 0.
    Bit 3 - Indicates if the message should continue to be transmitted if the
         long-term communications loss period (rsuLongCommLossTime) is
         exceeded. 0 indicates the message should continue to be transmitted.
         Default value is 0.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.4.2.1.7"
::= { rsuIFMStatusEntry 7 }
```

5.5.2.8 Forward Message Payload

```
rsuIFMPayload OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(0..2302))
    MAX-ACCESS   read-create
    STATUS       current
```

© 2020 AASHTO / ITE / NEMA

```
    DESCRIPTION  "<Definition> Payload of Immediate Forward message. Length
         limit derived from IEEE1609dot3-MIB. For SAE J2735-201603 messages,
         this object is the UPER encoded MessageFrame. This payload remains
         in this object until replaced by another payload.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.4.2.1.8"
::= { rsuIFMStatusEntry 8 }
```

5.6 Received Messages

```
rsuReceivedMsg OBJECT IDENTIFIER ::= { rsu 5 }
```

5.6.1 Maximum Number of Messages

```
maxRsuReceivedMsgs OBJECT-TYPE
    SYNTAX       Integer32 (1..255)
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> The maximum number of received message types
         (from the V2X interface), times and destinations for forwarding this
         Roadside Unit supports. This object indicates the maximum rows which
         appears in the rsuReceivedMsgTable object.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.5.1"
::= { rsuReceivedMsg 1 }
```

5.6.2 Received Messages Table

```
rsuReceivedMsgTable OBJECT-TYPE
    SYNTAX       SEQUENCE OF RsuReceivedMsgEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Contains the PSID being forwarded to a network
         host, the IP Address and port number of the destination host, as
         well as other configuration parameters as defined.
    <TableType>  dynamic
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.5.2"
::= { rsuReceivedMsg 2 }

rsuReceivedMsgEntry OBJECT-TYPE
    SYNTAX       RsuReceivedMsgEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> A row describing the RSU Message Forwarding
         types.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.5.2.1"
    INDEX        { rsuReceivedMsgIndex }
    ::= { rsuReceivedMsgTable 1 }

RsuReceivedMsgEntry ::= SEQUENCE {
    rsuReceivedMsgIndex              RsuTableIndex,
    rsuReceivedMsgPsid               RsuPsidTC,
    rsuReceivedMsgDestIpAddr         DisplayString,
    rsuReceivedMsgDestPort           Integer32,
    rsuReceivedMsgProtocol           INTEGER,
    rsuReceivedMsgRssi               Integer32,
    rsuReceivedMsgInterval           Integer32,
    rsuReceivedMsgDeliveryStart      DateAndTime,
```

 © 2020 AASHTO / ITE / NEMA

```
    rsuReceivedMsgDeliveryStop       DateAndTime,
    rsuReceivedMsgStatus             RowStatus,
    rsuReceivedMsgSecure             INTEGER,
    rsuReceivedMsgAuthMsgInterval    Integer32  }
```

5.6.2.1 Received Message Index

```
rsuReceivedMsgIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Message Forward Message Table Index. This
         value shall not exceed maxRsuReceivedMsgs.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.5.2.1.1"
::= { rsuReceivedMsgEntry 1 }
```

5.6.2.2 Received Message PSID

```
rsuReceivedMsgPsid OBJECT-TYPE
    SYNTAX       RsuPsidTC
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> The Provider Service Identifier (PSID) of a
         Message Received by the RSU via the V2X Interface to be forwarded.
         The current PSID assignments can be found at
         https://standards.ieee.org/products-
         services/regauth/psid/public.html.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.5.2.1.2"
::= { rsuReceivedMsgEntry 2 }
```

5.6.2.3 Received Message Destination Address

```
rsuReceivedMsgDestIpAddr OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..64))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Destination Server IP address to forward the
         message received by the RSU over the V2X Interface. For an IPv4
         remote destination, this address can be represented as an IPv4 quad-
         dotted IP address, for example, 192.33.44.235. For IPv6 remote
         destination, this address can be represented as zero-compressed
         simplified IPv6 address, for example 2031:0:130F::9C0:876A:130B.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.5.2.1.3"
::= { rsuReceivedMsgEntry 3 }
```

5.6.2.4 Received Message Destination Port

```
rsuReceivedMsgDestPort OBJECT-TYPE
    SYNTAX       Integer32 (1024..65535)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Destination Server Port Number to forward the
         message received by the RSU over the V2X Interface.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.5.2.1.4"
::= { rsuReceivedMsgEntry 4 }
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

5.6.2.5 Received Message Destination Protocol

```
rsuReceivedMsgProtocol OBJECT-TYPE
    SYNTAX       INTEGER { other (1), udp (2) }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Transport Protocol between RSU and Server to
         forward the message received by the RSU over the V2X Interface. The
         entire WSMP payload, including certificates and signature unless
         indicated by the rsuReceivedMsgSecure object, are to be forwarded.

         If udp is selected, the message contains the binary data (payload)
         defined by rsuReceivedMsgSecure.

         A SET to a value of 'other' shall return a badValue error.

         NOTE: If other is selected, this object allows for future
         extensions, possibly tcp.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.5.2.1.5"
    DEFVAL { udp }
::= { rsuReceivedMsgEntry 5 }
```

5.6.2.6 Received Message Minimum Signal Strength

```
rsuReceivedMsgRssi OBJECT-TYPE
    SYNTAX       Integer32 (-100..-60)
    UNITS        "dBm"
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Minimum Received Signal Strength Level (in dbm
         units) of the SAE J2735 message received by the RSU over the V2X
         Interface before forwarding to the Server.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.5.2.1.6"
::= { rsuReceivedMsgEntry 6 }
```

5.6.2.7 Received Message Forwarding Interval

```
rsuReceivedMsgInterval OBJECT-TYPE
    SYNTAX       Integer32 (0..10)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Interval with which RSU forwards messages
         received by the RSU over the V2X Interface to Server. For example, a
         value of 3 indicates every 3rd message received is forwarded (33% of
         the messages received). A value of 0 disables the message forward
         for this particular entry.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.5.2.1.7"
::= { rsuReceivedMsgEntry 7 }
```

5.6.2.8 Received Message Forwarding Start Time

```
rsuReceivedMsgDeliveryStart OBJECT-TYPE
    SYNTAX       DateAndTime
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Start time for RSU to start forwarding SAE
         J2735 Messages to Server in UTC. DateAndTime is of length 8 octets.
```

 © 2020 AASHTO / ITE / NEMA

```
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.5.2.1.8"
::= { rsuReceivedMsgEntry 8 }
```

5.6.2.9 Received Message Forwarding Stop Time

```
rsuReceivedMsgDeliveryStop OBJECT-TYPE
    SYNTAX       DateAndTime
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Stop time for RSU to stop forwarding SAE J2735
         Messages to Server in UTC. DateAndTime is of length 8 octets.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.5.2.1.9"
::= { rsuReceivedMsgEntry 9 }
```

5.6.2.10 Received Message Status

```
rsuReceivedMsgStatus OBJECT-TYPE
    SYNTAX       RowStatus
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Create (4) and destroy (6) row entry.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.5.2.1.10"
::= { rsuReceivedMsgEntry 10 }
```

5.6.2.11 Received Message Forward Secure Option

```
rsuReceivedMsgSecure OBJECT-TYPE
    SYNTAX       INTEGER (0..1)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> A value of 0 indicates the RSU is to forward
         only the WSM message payload without security headers. Specifically
         this means that either of the following is forwarded, depending on
         whether the message is signed (a) or unsigned (b): (a)
         Ieee1609Dot2Data.signedData.tbsData.payload.data.unsecuredData or
         (b) Ieee1609Dot2Data.unsecuredData.

         A value of 1 indicates the RSU is to forward the entire WSM
         including the security headers. Specifically this means that the
         entire Ieee1609Dot2Data frame is forwarded in COER format.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.5.2.1.11"
::= { rsuReceivedMsgEntry 11 }
```

5.6.2.12 Received Message Forward Secure Interval

```
rsuReceivedMsgAuthMsgInterval OBJECT-TYPE
    SYNTAX       Integer32 (0..10)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Interval with which the RSU authenticates
         messages received from a specific device over the V2X Interface and
         to be forwarded to the Server (as controlled by
         rsuDsrcFwdMsgInterval). If enabled, the RSU authenticates the first
         valid (e.g., as defined by rsuDsrcFwdRssi, rsuDsrcFwdDeliveryStart,
         rsuDsrcFwdDeliveryStop for this row) message received from a
         specific device. For a value of 4, the RSU then authenticates every
```

© 2020 AASHTO / ITE / NEMA

```
        4th message (after the first message) for that specific device that
        is marked for forwarding (as determined by rsuDsrcFwdMsgInterval). A
        value of 0 disables authentication of message to be forward for this
        particular entry.

        For example, an RSU receives 12 messages that satisfies the criteria
        for this row (rsuDsrcFwdPsid, rsuDsrcFwdRssi,
        rsuDsrcFwdDeliveryStart, rsuDsrcFwdDeliveryStop). Messages 1, 2, 5,
        6, 7, 10 and 12 are from device A and messages 3, 4, 8, 9 and 11 are
        from device B. Assuming rsuDsrcFwdMsgInterval has a value of 2, only
        messages 1, 3, 5, 7, 9, and 11 are 'marked' for forwarding. Of these
        messages, only messages 1 (the first message from device A), 3 (the
        first message from device B), 7 (the 2nd message from device A after
        the first message), and 11 (the 2nd message from device B after the
        first message) are authenticated.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.5.2.1.12"
::= { rsuReceivedMsgEntry 12 }
```

5.7 GNSS Output

```
rsuGnssOutput OBJECT IDENTIFIER ::= { rsu 6 }
```

5.7.1 GNSS Output Port

```
rsuGnssOutputPort OBJECT-TYPE
    SYNTAX       Integer32 (1024..65535)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> GNSS Out External Server Port Number.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.6.1"
    DEFVAL       { 5115 }
::= { rsuGnssOutput 1 }
```

5.7.2 GNSS Output Address

```
rsuGnssOutputAddress OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..64))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Remote host address to which to transmit the
         GNSS string. For an IPv4 remote destination, this address can be
         represented as an IPv4 quad-dotted IP address, for example,
         192.33.44.235. For IPv6 remote destination, this address can be
         represented as zero-compressed simplified IPv6 address, for example
         2031:0:130F::9C0:876A:130B.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.6.2"
::= { rsuGnssOutput 2 }
```

5.7.3 GNSS Output Interface Description

```
rsuGnssOutputInterface OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..100))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Local interface on the RSU which to output the
         GNSS string. E.g., eth0, eth1.
```

 © 2020 AASHTO / ITE / NEMA

```
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.6.3"
::= { rsuGnssOutput 3 }
```

5.7.4 GNSS Output Interval

```
rsuGnssOutputInterval OBJECT-TYPE
    SYNTAX       Integer32 (0..18000)
    UNITS        "second"
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Interval at which to transmit the
         rsuGNSSOutputString value to the remote host in seconds. A value of
         0 indicates the transmission is disabled.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.6.4"
    DEFVAL       { 1 }
::= { rsuGnssOutput 4 }
```

5.7.5 GNSS Data Output

```
rsuGnssOutputString OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..100))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Contains NMEA 0183 GPGGA or GNGGA output
         string including the $ starting character and the ending <CR><LF>.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.6.5"
::= { rsuGnssOutput 5 }
```

5.7.6 GNSS Reported Latitude

```
rsuGnssLat OBJECT-TYPE
    SYNTAX       Integer32 (-900000000..900000001)
    UNITS        "tenth of a microdegree"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Contains the actual GNSS latitude for
         validation of reference GNSS latitude (rsuLocationLat) in 10^-7
         degrees. The value 900000001 represents unknown.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.6.6"
    DEFVAL { 900000001 }
::= { rsuGnssOutput 6 }
```

5.7.7 GNSS Reported Longitude

```
rsuGnssLon OBJECT-TYPE
    SYNTAX       Integer32 (-1800000000..1800000001)
    UNITS        "tenth of a microdegree"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Contains the actual GNSS longitude for
         validation of reference GNSS longitude (rsuLocationLong) in 10^-7
         degrees. The value 1800000001 represents unknown.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.6.7"
    DEFVAL { 1800000001 }
::= { rsuGnssOutput 7 }
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

5.7.8 GNSS Reported Elevation

```
rsuGnssElv OBJECT-TYPE
    SYNTAX       Integer32 (-100000..1000001)
    UNITS        "centimeter"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Contains the actual GNSS elevation for
         validation of reference GNSS elevation (rsuLocationElv) in
         centimeters above the reference ellipsoid as defined by the WGS-84.
         The value of 1000001 represents unknown.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.6.8"
    DEFVAL { 1000001 }
::= { rsuGnssOutput 8 }
```

5.7.9 GNSS Allowable Location Deviation

```
rsuGnssMaxDeviation OBJECT-TYPE
    SYNTAX       Integer32 (0..20000)
    UNITS        "meter"
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Contains the maximum allowable deviation
         between the actual 2D GNSS coordinates of the RSU (rsuGnssLat,
         rsuGnssLon) and the reference GNSS coordinates (rsuLocationLat,
         rsuLocationLon). A value of 0 disables this feature.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.6.9"
::= { rsuGnssOutput 9 }
```

5.7.10 GNSS Location Deviation

```
rsuLocationDeviation OBJECT-TYPE
    SYNTAX       Integer32 (0..20001)
    UNITS        "meter"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> The 2D deviation, in centimeters, between the
         reported GNSS coordinates (rsuGnssLat, rsuGnssLon) and the RSU's
         reference location (rsuLocationLat, rsuLocationLon).
    <Valid Value Rule> Values of 0 to 19,999 provides a range from 0
         centimeters to 19,999 meters. The value of 20,000 represents 20,000
         meters or more. The value of 200001 represents unknown.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.6.10"
::= { rsuGnssOutput 10 }
```

5.7.11 RSU Position Error

```
rsuGnssPositionError OBJECT-TYPE
    SYNTAX       Integer32 (0..200001)
    UNITS        "tenth of a meter"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "<Definition> Contains the estimated average position error
         in centimeters, at 67% confidence ((1) standard deviation). Values
         of 0 to 200,000 provides a range from 0 meters to 20,000 meters. The
         value of 200,001 represents unknown.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.6.11"
```

 © 2020 AASHTO / ITE / NEMA

```
    DEFVAL { 200001 }
::= { rsuGnssOutput 11 }
```

5.8 Interface Log

```
rsuInterfaceLog OBJECT IDENTIFIER ::= { rsu 7 }
```

5.8.1 Maximum Number of Interface Logs

```
maxRsuInterfaceLogs OBJECT-TYPE
    SYNTAX       Integer32 (1..255)
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> The maximum number of active Interface Logs
         this Roadside Unit supports. This object indicates the maximum rows
         which appears in the rsuInterfaceLogTable object.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.7.1"
::= { rsuInterfaceLog 1 }
```

5.8.2 Interface Log Table

```
rsuInterfaceLogTable OBJECT-TYPE
    SYNTAX       SEQUENCE OF RsuInterfaceLogEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Provides configuration information for
         capturing log files for a communication interface. The index
         represents the interface for which these configurations apply.
    <TableType> dynamic
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.7.2"
::= { rsuInterfaceLog 2 }

rsuInterfaceLogEntry OBJECT-TYPE
    SYNTAX       RsuInterfaceLogEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> A row describing RSU Interface Log.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.7.2.1"
    INDEX   { rsuIfaceLogIndex }
::= {rsuInterfaceLogTable 1 }

RsuInterfaceLogEntry ::= SEQUENCE {
    rsuIfaceLogIndex             RsuTableIndex,
    rsuIfaceGenerate             INTEGER,
    rsuIfaceMaxFileSize          Integer32,
    rsuIfaceMaxFileTime          Integer32,
    rsuIfaceLogByDir             INTEGER,
    rsuIfaceName                 DisplayString,
    rsuIfaceStoragePath          DisplayString,
    rsuIfaceLogName              DisplayString,
    rsuIfaceLogStart             DateAndTime,
    rsuIfaceLogStop              DateAndTime,
    rsuIfaceLogOptions           BITS,
    rsuIfaceLogStatus            RowStatus }
```

© 2020 AASHTO / ITE / NEMA

5.8.2.1 Interface Log Index

```
rsuIfaceLogIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Interface Logging Index. This value shall not
         exceed maxRsuInterfaceLogs.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.7.2.1.1"
::= { rsuInterfaceLogEntry 1 }
```

5.8.2.2 Interface Log Enable

```
rsuIfaceGenerate OBJECT-TYPE
    SYNTAX       INTEGER { off (0),
                           on (1) }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Set this bit to Enable / Disable interface
         logging for this row. 1 is to enable interface logging.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.7.2.1.2"
::= { rsuInterfaceLogEntry 2 }
```

5.8.2.3 Interface Log Maximum File Size

```
rsuIfaceMaxFileSize OBJECT-TYPE
    SYNTAX       Integer32 (1..40)
    UNITS        "megabyte"
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Maximum Interface Log File Size in megabytes,
         default is 5.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.7.2.1.3"
    DEFVAL       { 5 }
::= { rsuInterfaceLogEntry 3 }
```

5.8.2.4 Interface Log Maximum Collection Time

```
rsuIfaceMaxFileTime OBJECT-TYPE
    SYNTAX       Integer32 (1..48)
    UNITS        "hour"
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Maximum Collection time for Interface Logging
         in hours, default is 24.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.7.2.1.4"
::= { rsuInterfaceLogEntry 4 }
```

5.8.2.5 Interface Log Direction Separation

```
rsuIfaceLogByDir OBJECT-TYPE
    SYNTAX       INTEGER { inboundOnly (1),
                 outboundOnly (2),
                 biSeparate (3),
                 biCombined (4) }
    MAX-ACCESS   read-create
    STATUS       current
```

 © 2020 AASHTO / ITE / NEMA

```
    DESCRIPTION  "<Definition> Sets which direction of communications traffic
         to capture in the interface data log. biSeparate (3) indicates both
         directions are to be captured but in separate interface data log
         files, while biCombined (4) indicates both directions are to be
         captured in the same interface data log file.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.7.2.1.5"
::= { rsuInterfaceLogEntry 5 }
```

5.8.2.6 Interface Name

```
rsuIfaceName OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..127))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Identifies the name of the interface for which
         the logs defined by this row are to be managed. E.g., wlan0, gnss,
         dsrc.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.7.2.1.6"
::= { rsuInterfaceLogEntry 6 }
```

5.8.2.7 Interface Log Storage Path

```
rsuIfaceStoragePath OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(1..255))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Indicates the storage path of the interface
         file logs. The path indicated here shall be relative to the base
         directory (see rsuSysDir). The base directory is specified by the
         string '/' (one forward slash). A subdirectory from the base may be
         specified by the string '/subdir'.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.7.2.1.7"
::= { rsuInterfaceLogEntry 7 }
```

5.8.2.8 Interface Log Name

```
rsuIfaceLogName OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(12..172))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Indicates the filename used when storing new
         interface data logs. This parameter shall be in the format
         <identifier>_<interface>_<direction>_<time> and contain only the
         following case-sensitive field names enclosed in chevrons (<>):
           <identifier>: Identifier of the RSU. See rsuID.
           <interface>: Identifier of the interface. See rsuIfaceName.
           <direction>: Direction of communications. In for Inbound, Out for
         Outbound), and Both for inbound and outbound.
           <time>: In UTC. The format is YYYYMMDD_hhmmss, where YYYY is the
         four-digit year, MM is the two-digit month, DD is the two-digit day,
         hh is the two-digit hour, mm is the two-digit minute, and ss is the
         two-digit seconds.

         Example: If the rsuID = rsu1, rsuIfaceName = dsrc1, both directions
         are collected in the same file, and the date and time the file was
```

© 2020 AASHTO / ITE / NEMA

```
         created is January 3, 2019, at 01:35:03, the filename would be
         rsu1_dsrc1_Both_20190103_013503.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.7.2.1.8"
::= { rsuInterfaceLogEntry 8 }
```

5.8.2.9 Interface Log Start Time

```
rsuIfaceLogStart OBJECT-TYPE
    SYNTAX       DateAndTime
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Interface Log start time in UTC. DateAndTime
         of length 8 octets.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.7.2.1.9"
::= { rsuInterfaceLogEntry 9 }
```

5.8.2.10 Interface Log Stop Time

```
rsuIfaceLogStop OBJECT-TYPE
    SYNTAX       DateAndTime
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Interface Log stop time in UTC. DateAndTime of
         length 8 octets.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.7.2.1.10"
::= { rsuInterfaceLogEntry 10 }
```

5.8.2.11 Interface Log Options

```
rsuIfaceLogOptions OBJECT-TYPE
    SYNTAX       BITS { diskFull(0),
                 deleteEntry(1) }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> A bit-mapped value as defined below for
         configuring the message.
         Bit 0        0=Delete oldest if disk full, 1=Stop if disk full
         Bit 1        0=DoNotDelete, 1=Delete data log

    Bit 0 - Indicates if the RSU is to delete the oldest interface data log
         file if the disk space for storing interface data logs is full, or
         to stop interface data logging. Default is to delete the oldest file
    Bit 1 - Indicates if the RSU is to delete the corresponding interface
         data log file when an entry is destroyed in the
         rsuInterfaceLogTable. Default is not to delete the log file.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.7.2.1.11"
::= { rsuInterfaceLogEntry 11 }
```

5.8.2.12 Interface Log Status

```
rsuIfaceLogStatus OBJECT-TYPE
    SYNTAX       RowStatus
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Create (4) and destroy (6) row entry.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.7.2.1.12"
```

 © 2020 AASHTO / ITE / NEMA

```
::= { rsuInterfaceLogEntry 12 }
```

5.9 Security

```
rsuSecurity OBJECT IDENTIFIER ::= { rsu 8 }
```

5.9.1 Security Credentials Request

```
rsuSecCredReq OBJECT-TYPE
    SYNTAX       Integer32 (0..8736)
    UNITS        "hour"
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Provides configuration parameters for when an
         RSU should request new 1609.2 security credentials in hours, before
         existing credentials expire. A value of 0 indicates disabled, so the
         RSU never updates its certificates globally.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.1"
    DEFVAL { 168 }
::= { rsuSecurity 1 }
```

5.9.2 Enrollment Certificate Status

```
rsuSecEnrollCertStatus OBJECT-TYPE
    SYNTAX       INTEGER { other (1),
                 unknown (2),
                 notEnrolled (3),
                 enrolled (4) }
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Provides the status of the enrollment
         certificates for the RSU.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.2"
::= { rsuSecurity 2 }
```

5.9.3 Enrollment Certificate Valid Region

```
rsuSecEnrollCertValidRegion OBJECT-TYPE
    SYNTAX       Integer32 (0..65535)
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Provides the valid region identifier, such as
         a country code, that the enrollment certificates for the RSU is
         valid for, or 0 for 'other'. For the United States, the country code
         is 840.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.3"
::= { rsuSecurity 3 }
```

5.9.4 Enrollment Certificate Source Domain

```
rsuSecEnrollCertUrl OBJECT-TYPE
    SYNTAX       Uri255
    MAX-ACCESS   read-only
    STATUS       current
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

```
    DESCRIPTION  "<Definition> Provides the domain resource locator (URL) of
         the Certificate Authority that is the source of the enrollment
         certificate.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.4"
::= { rsuSecurity 4 }
```

5.9.5 Enrollment Certificate Identifier

```
rsuSecEnrollCertId OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(1..255))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Provides the enrollment certificate identifier
         (hashID8).
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.5"
::= { rsuSecurity 5 }
```

5.9.6 Enrollment Certificate Expiration

```
rsuSecEnrollCertExpiration OBJECT-TYPE
    SYNTAX       DateAndTime
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Provides the date and time that the existing
         enrollment certificate expires. DateAndTime is of length 8 octets.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.6"
::= { rsuSecurity 6 }
```

5.9.7 Enrollment Certificate Source

```
rsuSecuritySource OBJECT-TYPE
    SYNTAX       INTEGER { other(1),
                 sCMS(2),
                 manual(3) }
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Indicates if the source of the enrollment
         certificate is from the Security Credential Management System (SCMS)
         or manually loaded.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.7"
::= { rsuSecurity 7 }
```

5.9.8 Application Certificate Source

```
rsuSecAppCertUrl OBJECT-TYPE
    SYNTAX       Uri1024
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Provides the domain resource locator (URL)
         from which to request new application certificates.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.8"
::= { rsuSecurity 8 }
```

5.9.9 Maximum Application Certificates

```
maxRsuSecAppCerts OBJECT-TYPE
```

 © 2020 AASHTO / ITE / NEMA

```
    SYNTAX       RsuTableIndex
    UNITS        "Application Certificates"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> The maximum number of application certificates
this Roadside Unit supports. This object indicates the maximum rows which
appears in the rsuSecAppCertTable object.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.8.9"
::= { rsuSecurity 9 }
```

5.9.10 Application Certificate Table

```
rsuSecAppCertTable OBJECT-TYPE
    SYNTAX       SEQUENCE OF RsuSecAppCertEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Provides status information about application
         certificates for the RSU.
    <TableType> static
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.10"
::= { rsuSecurity 10 }

rsuSecAppCertEntry OBJECT-TYPE
    SYNTAX       RsuSecAppCertEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> A row describing the status of an application
         certificate.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.10.1"
    INDEX   { rsuSecAppCertIndex }
::= { rsuSecAppCertTable 1 }

RsuSecAppCertEntry ::= SEQUENCE {
    rsuSecAppCertIndex           RsuTableIndex,
    rsuSecAppCertPsid            OCTET STRING,
    rsuSecAppCertState           INTEGER,
    rsuSecAppCertExpiration      Integer32,
    rsuSecAppCertReq             Integer32 }
```

5.9.10.1 Application Certificate Index

```
rsuSecAppCertIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Application Certificate Index. This value
         shall not exceed maxRsuSecAppCerts.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.10.1.1"
::= { rsuSecAppCertEntry 1 }
```

5.9.10.2 Application Certificate PSID

```
rsuSecAppCertPsid OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(1..255))
    MAX-ACCESS   read-only
    STATUS       current
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

```
    DESCRIPTION  "<Definition> Contains the PSIDs associated with this
         application certificate (up to 64). The PSID is formatted per
         IEEE1609.12-2016 Table 2 as P-encoded hex values. All PSIDs are to
         be padded to a 4-octet length. The current PSID assignments can be
         found at https://standards.ieee.org/products-
         services/regauth/psid/public.html.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.10.1.2"
::= { rsuSecAppCertEntry 2 }
```

5.9.10.3 Application Certificate State

```
rsuSecAppCertState OBJECT-TYPE
    SYNTAX       INTEGER { other (1),
                 valid (2),
                 notValid (3),
                 future (4) }
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Provides the status of the application
         certificates for the RSU. Validity check is based on geographic
         region and time.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.10.1.3"
::= { rsuSecAppCertEntry 3 }
```

5.9.10.4 Application Certificate Expiration

```
rsuSecAppCertExpiration OBJECT-TYPE
    SYNTAX       Integer32 (0..255)
    UNITS        "hour"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Provides the number of hours remaining before
         the existing application certificate expires.
         <Valid Value Rule> A value of 0 indicates the certificates expire
         that day, but have not expired yet. A value of 255 indicates the
         certificates have expired. A value of 254 indicates the expiration
         date is 254 hours or longer.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.10.1.4"
::= { rsuSecAppCertEntry 4 }
```

5.9.10.5 Application Certificate Request

```
rsuSecAppCertReq OBJECT-TYPE
    SYNTAX       Integer32 (0..65535)
    UNITS        "hour"
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Provides configuration parameters for when an
         RSU should request new 1609.2 security credentials in hours before
         the application certificate expire.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.10.1.5"
::= { rsuSecAppCertEntry 5 }
```

 © 2020 AASHTO / ITE / NEMA

5.9.11 Certificate Revocation List Source

```
rsuSecCertRevocationUrl OBJECT-TYPE
    SYNTAX       Uri255
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Provides the domain resource locator (URL)
         from which to request updated certificate revocation lists.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.11"
::= { rsuSecurity 11 }
```

5.9.12 Certificate Revocation List Update Time

```
rsuSecCertRevocationTime OBJECT-TYPE
    SYNTAX       DateAndTime
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Provides the date and time that the
         certificate revocation list was last updated. DateAndTime is of
         length 8 octets.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.12"
::= { rsuSecurity 12 }
```

5.9.13 Certificate Revocation Update Interval

```
rsuSecCertRevocationInterval OBJECT-TYPE
    SYNTAX       Integer32 (0..255)
    UNITS        "hour"
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Time interval in hours between requests for an
         updated certificate revocation list from the Certificate Authority.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.13"
    DEFVAL { 24 }
::= { rsuSecurity 13 }
```

5.9.14 Certificate Revocation List Command

```
rsuSecCertRevocationUpdate OBJECT-TYPE
    SYNTAX       INTEGER (0..1)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> This object when set to TRUE (one) shall cause
         the roadside unit to initiate a request to update the certificate
         revocation list for the RSU. This object shall automatically return
         to FALSE (zero) after the request has been transmitted.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.14"
::= { rsuSecurity 14 }
```

5.9.15 Maximum Number of Security Profile Entries

```
maxRsuSecProfiles OBJECT-TYPE
    SYNTAX       Integer32 (1..255)
    MAX-ACCESS   read-only
    STATUS       current
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

```
    DESCRIPTION  "<Definition> The maximum number of security profile entries
this Roadside Unit supports. This object indicates the maximum rows which
appears in the rsuSecProfileTable object.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.15"
::= { rsuSecurity 15 }
```

5.9.16 Security Profiles

```
rsuSecProfileTable OBJECT-TYPE
    SYNTAX       SEQUENCE OF RsuSecProfileEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Provides information about the security
        profiles on the RSU.
    <TableType> static
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.16"
::= { rsuSecurity 16 }

rsuSecProfileEntry OBJECT-TYPE
    SYNTAX       RsuSecProfileEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> A row describing the parameters for a security
        profile.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.16.1"
    INDEX   { rsuSecProfileIndex }
::= { rsuSecProfileTable 1 }

RsuSecProfileEntry ::= SEQUENCE {
      rsuSecProfileIndex       RsuTableIndex,
      rsuSecProfileName        DisplayString,
      rsuSecProfileDesc        DisplayString }
```

5.9.16.1 RSU Security Profile Index

```
rsuSecProfileIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> RSU Security Profile Index. This value shall
        not exceed maxRsuSecProfiles.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.16.1.1"
::= { rsuSecProfileEntry 1 }
```

5.9.16.2 RSU Security Profile Name

```
rsuSecProfileName OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(1..127))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Name of the security profile.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.16.1.2"
::= { rsuSecProfileEntry 2 }
```

 © 2020 AASHTO / ITE / NEMA

5.9.16.3 RSU Security Profile Description

```
rsuSecProfileDesc OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..255))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Description of the security profile.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.8.16.1.3"
::= { rsuSecProfileEntry 3 }
```

5.10 WAVE Service Advertisement

```
rsuWsaConfig OBJECT IDENTIFIER ::= { rsu 9 }
```

5.10.1 Maximum Number of WSA Services

```
maxRsuWsaServices OBJECT-TYPE
    SYNTAX       Integer32 (1..255)
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> The maximum number of WAVE service
         advertisements this Roadside Unit supports. This object indicates
         the maximum rows which appears in the rsuWsaServiceTable and
         rsuWsaChannelTable object.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.1"
::= { rsuWsaConfig 1 }
```

5.10.2 WAVE Service Advertisement Service Table

```
rsuWsaServiceTable OBJECT-TYPE
    SYNTAX       SEQUENCE OF RsuWsaServiceEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Holds general service configuration parameters
        for the RSU WAVE Service Advertisement.
    <TableType> dynamic
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.2"
::= { rsuWsaConfig 2 }

rsuWsaServiceEntry OBJECT-TYPE
    SYNTAX       RsuWsaServiceEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> A row describing a RSU WSA Service.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.2.1"
    INDEX   { rsuWsaIndex }
::= {rsuWsaServiceTable 1 }

RsuWsaServiceEntry ::= SEQUENCE {
    rsuWsaIndex                  RsuTableIndex,
    rsuWsaPsid                   RsuPsidTC,
    rsuWsaPriority               Integer32,
    rsuWsaPSC                    OCTET STRING,
    rsuWsaIpAddress              DisplayString,
    rsuWsaPort                   Integer32,
    rsuWsaChannel                Integer32,
    rsuWsaStatus                 RowStatus,
```

© 2020 AASHTO / ITE / NEMA

```
    rsuWsaMacAddress              MacAddress,
    rsuWsaOptions                 BITS,
    rsuWsaRcpiThreshold           Integer32,
    rsuWsaCountThreshold          Integer32,
    rsuWsaCountThresholdInterval  Integer32,
    rsuWsaRepeatRate              Integer32,
    rsuWsaAdvertiserIdentifier    OCTET STRING,
    rsuWsaEnable                  INTEGER  }
```

5.10.2.1 WAVE Service Advertisement Index

```
rsuWsaIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> WSA Service Index. This value shall not exceed
        the maxRsuWsaServices object value.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.2.1.1"
::= { rsuWsaServiceEntry 1 }
```

5.10.2.2 WAVE Service Advertisement PSID

```
rsuWsaPsid OBJECT-TYPE
    SYNTAX       RsuPsidTC
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> WSA Service PSID.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.2.1.2"
    REFERENCE "IEEE 1609.3-2016 dot3ProviderServiceIdentifier"
::= { rsuWsaServiceEntry 2 }
```

5.10.2.3 WAVE Service Advertisement Priority

```
rsuWsaPriority OBJECT-TYPE
    SYNTAX       Integer32 (0..7)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> User priority for which the WSA is
        transmitted. See IEEE 1609.3-2016 as a reference.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.2.1.3"
::= { rsuWsaServiceEntry 3 }
```

5.10.2.4 WAVE Service Advertisement Provider Service Context

```
rsuWsaPSC OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(0..31))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> WSA Service Specific Provider Context, 1-31
        octets. An octet string of SIZE(0) indicates to omit the PSC from the
        WSA.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.2.1.4"
    REFERENCE "IEEE 1609.3-2016 dot3ProviderServiceContext"
::= { rsuWsaServiceEntry 4 }
```

 © 2020 AASHTO / ITE / NEMA

5.10.2.5 WAVE Service Advertisement Application Host

```
rsuWsaIpAddress OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..64))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> IPv6 address of the service advertised by the
        WSA. For IPv6 remote destination, this address can be represented as
        zero-compressed simplified IPv6 address, for example
        2031:0:130F::9C0:876A:130B.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.2.1.5"
    REFERENCE "IEEE 1609.3-2016 dot3ProviderIpv6Address"
::= { rsuWsaServiceEntry 5 }
```

5.10.2.6 WAVE Service Advertisement Application Port

```
rsuWsaPort OBJECT-TYPE
    SYNTAX       Integer32 (1024..65535)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Port Number of the service advertised by the
        WSA.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.2.1.6"
    REFERENCE "IEEE 1609.3-2016 dot3ProviderServicePort"
::= { rsuWsaServiceEntry 6 }
```

5.10.2.7 WAVE Service Advertisement Application Channel

```
rsuWsaChannel OBJECT-TYPE
    SYNTAX       Integer32 (0..255)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> The channel number on which the WSA for the
        advertised service is provided. For DSRC radios in the United States,
        the transmission channel is from 172 to 184, as defined by IEEE
        802.11. For PC5 radios in the United States, the relationship between
        IEEE802.11 and 3GPP channel numbers is found in Table 7 of NTCIP 1218
        v01.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.2.1.7"
    REFERENCE "IEEE 1609.3-2016 dot3ProviderWsaChannelNumber"
::= { rsuWsaServiceEntry 7 }
```

5.10.2.8 WAVE Service Advertisement Status

```
rsuWsaStatus OBJECT-TYPE
    SYNTAX       RowStatus
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Create (4) or destroy (6) row entry.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.2.1.8"
::= { rsuWsaServiceEntry 8 }
```

5.10.2.9 WAVE Service Advertisement MAC Address

```
rsuWsaMacAddress OBJECT-TYPE
    SYNTAX       MacAddress
    MAX-ACCESS   read-create
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

```
    STATUS       current
    DESCRIPTION  "<Definition> MAC address of the server associated with the
        requested service.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.2.1.9"
    REFERENCE "IEEE 1609.3-2016 dot3ProviderMacAddress"
::= { rsuWsaServiceEntry 9 }
```

5.10.2.10 WAVE Service Advertisement Options

```
rsuWsaOptions OBJECT-TYPE
    SYNTAX       BITS { secured (0),
                 wra (1),
                 repeatRate (2),
                 twoDLocation (3),
                 threeDLocation (4),
                 rcpiThreshold (5) }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> A bit-mapped value as defined below for
        configuring the transmitted WSA.
        BIT 0    0=unsecuredWsa, 1=securedWsa
        BIT 1    WRA 0=not transmitted, 1=transmitted
        BIT 2    Repeat Rate 0=not transmitted, 1=transmitted
        BIT 3    2DLocation 0=not transmitted, 1=transmitted
        BIT 4    3DLocation 0=not transmitted, 1=transmitted
        BIT 5    RcpiThreshold 0=not transmitted, 1=transmitted
        BIT 6    Reserved
        BIT 7    Reserved

    Bit 0 - Indicates if security processing to be applied to the transmitted
         WSA.
    Bit 1 - Indicates if the WSA should include the WAVE Routing
         Advertisement.
    Bit 2 - Indicates if the Repeat Rate is transmitted in the WSA Header.
    Bit 3 - Indicates if the 2DLocation is transmitted in the WSA Header. The
         2DLocation value is defined by rsuLocationLat and rsuLocationLong.
         If Bit 4=1, then the 3DLocation value is transmitted and 2DLocation
         is not.
    Bit 4 - Indicates if the 3DLocation is transmitted in the WSA Header. The
         2DLocation value is defined by rsuLocationLat, rsuLocationLong and
         rsuLocationElv.
    Bit 5 - Indicates if the RcpiThreshold value is transmitted in the WSA
         Header.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.2.1.10"
    REFERENCE "IEEE 1609.3-2016 dot3WsaType, IEEE 1609.3-2016
        dot3ProviderIpService, IEEE 1609.3-2016 dot3ProviderRepeatRate, IEEE
        1609.3-2016 dot3ProviderRcpiThreshold "
::= { rsuWsaServiceEntry 10 }
```

5.10.2.11 WAVE Service Advertisement RCPI Threshold

```
rsuWsaRcpiThreshold OBJECT-TYPE
    SYNTAX       Integer32 (0..255)
    MAX-ACCESS   read-create
    STATUS       current
```

 © 2020 AASHTO / ITE / NEMA

```
    DESCRIPTION  "<Definition> The recommended power of received WSAs for
        accepting the advertised service. Coded per IEEE Std 802.11-
        2012/18.3.10.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.2.1.11"
    REFERENCE "IEEE 1609.3-2016 dot3ProviderRcpiThreshold"
::= { rsuWsaServiceEntry 11 }
```

5.10.2.12 WAVE Service Advertisement Count Threshold

```
rsuWsaCountThreshold OBJECT-TYPE
    SYNTAX       Integer32 (0..255)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> The recommended number of received WSAs within
        the number of 100 ms intervals defined by
        rsuWsaCountThresholdInterval before accepting the advertised service.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.2.1.12"
    REFERENCE "IEEE 1609.3-2016 dot3ProviderWsaCountThreshold"
::= { rsuWsaServiceEntry 12 }
```

5.10.2.13 WAVE Service Advertisement Count Interval

```
rsuWsaCountThresholdInterval OBJECT-TYPE
    SYNTAX       Integer32 (0..255)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION   "<Definition> The number of 100 millisecond intervals over
        which to count received WSAs before accepting the advertised service.
        Used with rsuWsaCountThreshold. A value of 0 indicates the WSA count
        threshold and WSA count threshold interval is not transmitted in the
        IEEE 1609.3 WSA header.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.2.1.13"
    REFERENCE "IEEE 1609.3-2016 dot3ProviderWsaCountThresholdInterval"
::= { rsuWsaServiceEntry 13 }
```

5.10.2.14 WAVE Service Advertisement Repeat Rate

```
rsuWsaRepeatRate OBJECT-TYPE
    SYNTAX       Integer32 (0..255)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION   "<Definition> The number of WAVE Service Advertisements to
        be transmitted each 5 seconds.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.2.1.14"
    REFERENCE "IEEE 1609.3-2016 dot3ProviderRepeatRate"
::= { rsuWsaServiceEntry 14 }
```

5.10.2.15 WAVE Service Advertiser Identifier

```
rsuWsaAdvertiserIdentifier OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(0..31))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION   "<Definition> A string identifying the service provider
        device that may be included in the WSA header. A string of SIZE (0)
```

© 2020 AASHTO / ITE / NEMA

```
        indicates to ignore this element and is not transmitted in the IEEE
        1609.3 WSA header.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.2.1.15"
    REFERENCE "IEEE 1609.3-2016 dot3AdvertiserIdentifier"
::= { rsuWsaServiceEntry 15 }
```

5.10.2.16 WAVE Service Advertisement Enable

```
rsuWsaEnable OBJECT-TYPE
    SYNTAX       INTEGER { disabled (0),
                           enabled (1) }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION   "<Definition> This object when set to TRUE (1) shall cause
        the Roadside Unit to perform a consistency check to confirm that the
        values in this row and the associated row in the rsuWsaChannelTable
        (See 5.10.4), as determined by the PSID (see rsuWsaChannelPsid), are
        valid. If the consistency check fails, the value of this object shall
        automatically return to FALSE (0), a genError is returned, and an
        error is logged.

        A value of 1 indicates that this WSA entry is enabled and should be
        broadcasted over the V2X Interface.

        A value of 0 indicates that this WSA entry is disabled and should not
        be broadcasted.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.2.1.16"
::= { rsuWsaServiceEntry 16 }
```

5.10.3 WAVE Service Advertisement Channel Table

```
rsuWsaChannelTable OBJECT-TYPE
    SYNTAX       SEQUENCE OF RsuWsaChannelEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Contains the desired channel configuration
        parameters for services to be advertised.
    <TableType> dynamic
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.3"
::= { rsuWsaConfig 3 }

rsuWsaChannelEntry OBJECT-TYPE
    SYNTAX       RsuWsaChannelEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> A row describing channel configuration for a
        service to be advertised.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.3.1"
    INDEX   { rsuWsaChannelIndex }
::= {rsuWsaChannelTable 1 }

RsuWsaChannelEntry ::= SEQUENCE {
    rsuWsaChannelIndex          RsuTableIndex,
    rsuWsaChannelPsid           RsuPsidTC,
    rsuWsaChannelNumber         Integer32,
    rsuWsaChannelTxPowerLevel   Integer32,
```

 © 2020 AASHTO / ITE / NEMA

```
    rsuWsaChannelAccess         INTEGER,
    rsuWsaChannelStatus         RowStatus }
```

5.10.3.1 WAVE Service Advertisement Channel Index

```
rsuWsaChannelIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> WSA Service Channel Index. This value shall
        not exceed the maxRsuWsaServices object value.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.3.1.1"
::= { rsuWsaChannelEntry 1 }
```

5.10.3.2 WAVE Service Advertisement Channel PSID

```
rsuWsaChannelPsid OBJECT-TYPE
    SYNTAX       RsuPsidTC
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> WSA Service PSID. This PSID (and this row)
         references all the services with the same PSID in 5.10.2 (See
         rsuWsaPsid).
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.3.1.2"
::= { rsuWsaChannelEntry 2 }
```

5.10.3.3 WAVE Service Advertisement Channel Number

```
rsuWsaChannelNumber OBJECT-TYPE
    SYNTAX       Integer32 (0..255)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Represents the channel number that the service
         is to be advertised on. For DSRC radios in the United States, the
         channel is from 172 to 184, as defined by IEEE 802.11. For PC5
         radios in the United States, the channel number is found in Table 7
         of NTCIP 1218 v01.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.3.1.3"
    REFERENCE    "IEEE 1609.3-2016 dot3ProviderChannelInfoChannelNumber"
::= { rsuWsaChannelEntry 3 }
```

5.10.3.4 WAVE Service Advertisement Transmit Power Level

```
rsuWsaChannelTxPowerLevel OBJECT-TYPE
    SYNTAX       Integer32 (-128..127)
    UNITS        "dBm"
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Represents the transmission power, in dBm, for
        the transmission of the service advertisement on the associated
        channel. Note that the Effective Isotropic Radiated Power (EIRP) is
        the sum of this object and the antenna gain (rsuAntGain).
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.3.1.4"
    REFERENCE    "IEEE 1609.3-2016 dot3ProviderChannelInfoTransmitPowerLevel"
::= { rsuWsaChannelEntry 4 }
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

5.10.3.5 WAVE Service Advertisement Transmit Channel Access

```
rsuWsaChannelAccess OBJECT-TYPE
    SYNTAX       INTEGER { both (0),
                 timeslot0 (1),
                 timeslot1 (2),
                 notUsed (3) }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Indicates the time slot(s) the device
        providing the application service is on the associated channel.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.3.1.5"
    REFERENCE    "IEEE 1609.3-2016 dot3ProviderChannelAccess"
::= { rsuWsaChannelEntry 5 }
```

5.10.3.6 WAVE Service Advertisement Channel Status

```
rsuWsaChannelStatus OBJECT-TYPE
    SYNTAX       RowStatus
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Create (4) or destroy (6) rows.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.3.1.6"
::= { rsuWsaChannelEntry 6 }
```

5.10.4 WAVE Service Advertisement Version

```
rsuWsaVersion OBJECT-TYPE
    SYNTAX       Integer32 (0..15)
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> WSA version as identified by IEEE 1609.3. The
        value is 3 for a WSA message conformant with IEEE 1609.3-2016.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.9.4"
    REFERENCE    "IEEE 1609.3-2016 8.2.2.2"
::= { rsuWsaConfig 4 }
```

5.11 WAVE Router Advertisement Configuration

```
rsuWraConfig OBJECT IDENTIFIER ::= { rsu 10 }
```

5.11.1 WAVE Router Advertisement Prefix

```
rsuWraIpPrefix OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..64))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> IPv6 address prefix of WRA Service Advertised.
        For IPv6 remote destination, this address can be represented as zero-
        compressed simplified IPv6 address, for example
        2031:0:130F::9C0:876A:130B.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.10.1"
    REFERENCE "IEEE 1609.3-2016 dot3ProviderWaveRoutingAdvertisementIpPrefix"
::= { rsuWraConfig 1 }
```

 © 2020 AASHTO / ITE / NEMA

5.11.2 WAVE Router Advertisement Prefix Length

```
rsuWraIpPrefixLength OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(1))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Length of IPv6 address prefix of WRA Service
        Advertised. A 64-bit prefix is '0x40', a 60-bit prefix is '0x3c' and
        a 52-bit prefix is '0x34'.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.10.2"
    REFERENCE "IEEE 1609.3-2016
        dot3ProviderWaveRoutingAdvertisementPrefixLength"
::= { rsuWraConfig 2 }
```

5.11.3 WAVE Router Advertisement Gateway

```
rsuWraGateway OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..64))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> IPv6 address of Gateway of WRA Service
        Advertised. For IPv6 remote destination, this address can be
        represented as zero-compressed simplified IPv6 address, for example
        2031:0:130F::9C0:876A:130B.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.10.3"
    REFERENCE "IEEE 1609.3-2016
        dot3ProviderWaveRoutingAdvertisementDefaultGateway"
::= { rsuWraConfig 3 }
```

5.11.4 WAVE Router Advertisement Primary DNS

```
rsuWraPrimaryDns OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..64))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Address of Primary DNS Server in WSA
        structure. For IPv6 remote destination, this address can be
        represented as zero-compressed simplified IPv6 address, for example
        2031:0:130F::9C0:876A:130B.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.10.4"
    REFERENCE "IEEE 1609.3-2016
        dot3ProviderWaveRoutingAdvertisementPrimaryDns"
::= { rsuWraConfig 4 }
```

5.11.5 WAVE Router Advertisement Secondary DNS

```
rsuWraSecondaryDns OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..64))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Address of Secondary DNS Server of WRA Service
        Advertised. For IPv6 remote destination, this address can be
        represented as zero-compressed simplified IPv6 address, for example
        2031:0:130F::9C0:876A:130B.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.10.5"
    REFERENCE "IEEE 1609.3-2016
        dot3ProviderWaveRoutingAdvertisementSecondaryDns"
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

```
::= { rsuWraConfig 5 }
```

5.11.6 WAVE Router Advertisement Gateway MAC

```
rsuWraGatewayMacAddress OBJECT-TYPE
    SYNTAX       MacAddress
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> MAC address of Gateway of WRA Service
        Advertised.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.10.6"
    REFERENCE "IEEE 1609.3-2016
        dot3ProviderWaveRoutingAdvertisementGatewayMACAddress"
::= { rsuWraConfig 6 }
```

5.11.7 WAVE Router Advertisement Lifetime

```
rsuWraLifetime OBJECT-TYPE
    SYNTAX       Integer32 (0..65535)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Router Lifetime. Lifetime is coded and
        interpreted as specified in IETF RFC 4861. A value of 0 should not
        be used for the default routers.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.10.7"
    REFERENCE "IEEE 1609.3-2016
        dot3ProviderWaveRoutingAdvertisementRouterLifetime"
::= { rsuWraConfig 7 }
```

5.12 Message Statistics

```
rsuMessageStats OBJECT IDENTIFIER ::= { rsu 11 }
```

5.12.1 Maximum Number of Message Counts by PSID

```
maxRsuMessageCountsByPsid OBJECT-TYPE
    SYNTAX       Integer32 (1..255)
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> The maximum number of monitored PSID messages
         this Roadside Unit supports. This object indicates the maximum rows
         which appears in the rsuMessageCountsByPsidTable object.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.11.1"
::= { rsuMessageStats 1 }
```

5.12.2 RSU Message Count Table

```
rsuMessageCountsByPsidTable OBJECT-TYPE
    SYNTAX       SEQUENCE OF RsuMessageCountsByPsidEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Provides a count of WAVE short messages sorted
        by PSID. Each row is a different PSID. A user can create or delete
        rows to tailor the list of monitored PSIDs.
    <TableType> dynamic
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.11.2"
```

Copy Per MIB Distribution Permission © 2020 AASHTO / ITE / NEMA

```
::= { rsuMessageStats 2 }

rsuMessageCountsByPsidEntry OBJECT-TYPE
    SYNTAX       RsuMessageCountsByPsidEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> A row describing the number of messages
        transmitted and received for a specific PSID.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.11.2.1"
    INDEX   { rsuMessageCountsByPsidIndex }
::= { rsuMessageCountsByPsidTable 1 }

RsuMessageCountsByPsidEntry ::= SEQUENCE {
    rsuMessageCountsByPsidIndex        RsuTableIndex,
    rsuMessageCountsByPsidId           RsuPsidTC,
    rsuMessageCountsByChannel          Integer32,
    rsuMessageCountsDirection          INTEGER,
    rsuMessageCountsByPsidTime         DateAndTime,
    rsuMessageCountsByPsidCounts       Counter32,
    rsuMessageCountsByPsidRowStatus    RowStatus  }
```

5.12.2.1 RSU Message Counter Index

```
rsuMessageCountsByPsidIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Message Transmission Counter Index. This value
        shall not exceed maxRsuMessageCountsByPsid.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.11.2.1.1"
::= { rsuMessageCountsByPsidEntry 1 }
```

5.12.2.2 RSU Message Counter Provider Service Identifier

```
rsuMessageCountsByPsidId OBJECT-TYPE
    SYNTAX       RsuPsidTC
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Represents the Provider Service Identifier
        (PSID) for the number of messages being reported. A value of 0x00
        indicates messages with any PSID is to be reported.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.12.2.1.2"
::= { rsuMessageCountsByPsidEntry 2 }
```

5.12.2.3 RSU Message Counter Channel

```
rsuMessageCountsByChannel OBJECT-TYPE
    SYNTAX       Integer32 (0..255)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Represents the V2X Channel for the number of
        messages being reported. A value of 0 indicates all channels are
        being reported.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.11.2.1.3"
::= { rsuMessageCountsByPsidEntry 3 }
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

5.12.2.4 RSU Message Counter Direction

```
rsuMessageCountsDirection OBJECT-TYPE
    SYNTAX       INTEGER { inbound(1),
                 outbound(2),
                 bothDir(3) }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Represents the direction of messages exchanged
        over the V2X Interface to be recorded. Inbound indicates only
        messages transmitted by the RSU over the V2X Interface is to be
        counted, while outbound indicates only messages received by the RSU
        over the V2X Interface is counted.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.11.2.1.4"
::= { rsuMessageCountsByPsidEntry 4 }
```

5.12.2.5 RSU Message Start Time

```
rsuMessageCountsByPsidTime OBJECT-TYPE
    SYNTAX       DateAndTime
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Contains the time the message counter began
        for this row. If this object is SET by a user, this is the start time
        to begin the message count. Otherwise, the system uses the time the
        RSU was last rebooted. DateAndTime is of length 8 octets.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.11.2.1.5"
::= { rsuMessageCountsByPsidEntry 5 }
```

5.12.2.6 RSU Message Counter

```
rsuMessageCountsByPsidCounts OBJECT-TYPE
    SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Contains the number of messages that have
        exchanged since the RSU was powered on.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.11.2.1.6"
::= { rsuMessageCountsByPsidEntry 6 }
```

5.12.2.7 RSU Message Counter Status

```
rsuMessageCountsByPsidRowStatus OBJECT-TYPE
    SYNTAX       RowStatus
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> RowStatus as defined in RFC2579 with minimum
        support for active = 1, notInService = 2, notReady = 3, createAndGo =
        4 or destroy = 6.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.11.2.1.7"
::= { rsuMessageCountsByPsidEntry 7 }
```

5.13 Systems Statistics

```
rsuSystemStats OBJECT IDENTIFIER ::= { rsu 12 }
```

 © 2020 AASHTO / ITE / NEMA

5.13.1 Time Since RSU Powered On

```
rsuTimeSincePowerOn OBJECT-TYPE
    SYNTAX       Counter32
    UNITS        "second"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Contains the total number of seconds that the
        system has been operational (i.e., in Operate or Standby states)
        since the RSU was last powered on.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.12.1"
::= { rsuSystemStats 1 }
```

5.13.2 RSU Internal Temperature

```
rsuIntTemp OBJECT-TYPE
    SYNTAX       Integer32 (-101..100)
    UNITS        "degree Celsius"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Contains the internal temperature of the RSU
        in degrees Celsius. A value of -101 indicates unknown.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.12.2"
    DEFVAL       { -101 }
::= { rsuSystemStats 2 }
```

5.13.3 RSU Internal Temperature - Low Temperature Warning

```
rsuIntTempLowThreshold OBJECT-TYPE
    SYNTAX       Integer32 (-101..100)
    UNITS        "degree Celsius"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Indicates the low value of the temperature, in
        degrees Celsius, associated with the internal temperature sensor
        below which would generate a notification. This value should not be
        higher than the value of the rsuIntTempHighThreshold object. A value
        of -101 indicates unknown.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.12.3"
    DEFVAL       { -101 }
::= { rsuSystemStats 3 }
```

5.13.4 RSU Internal Temperature - High Temperature Warning

```
rsuIntTempHighThreshold OBJECT-TYPE
    SYNTAX       Integer32 (-101..100)
    UNITS        "degree Celsius"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Indicates the high value of the temperature,
        in degrees Celsius, associated with the internal temperature sensor
        above which would generate a notification. This value should not be
        lower than the value of the rsuIntTempLowThreshold object. A value of
        -101 indicates unknown.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.12.4"
    DEFVAL       { -101 }
::= { rsuSystemStats 4 }
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

5.13.5 Maximum Number of Communications Range Entries

```
maxRsuCommRange OBJECT-TYPE
    SYNTAX       Integer32 (1..255)
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> The maximum number of communications range
         entries this Roadside Unit supports. This object indicates the
         maximum rows which appears in the rsuCommRangeTable object.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.12.5"
::= { rsuSystemStats 5 }
```

5.13.6 RSU Communications Range Table

```
rsuCommRangeTable OBJECT-TYPE
    SYNTAX       SEQUENCE OF RsuCommRangeEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Provides statistics on the RF communications
        range for a V2X radio using messages validated by security. Each row
        is a different sector and/or vehicle type.
    <TableType> dynamic
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.12.6"
::= { rsuSystemStats 6 }

rsuCommRangeEntry OBJECT-TYPE
    SYNTAX       RsuCommRangeEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> A row describing the RF communications range
        for a sector.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.12.6.1"
    INDEX   { rsuCommRangeIndex }
::= { rsuCommRangeTable 1 }

RsuCommRangeEntry ::= SEQUENCE {
      rsuCommRangeIndex       RsuTableIndex,
      rsuCommRangeSector      Integer32,
      rsuCommRangeMsgId       Integer32,
      rsuCommRangeFilterType  INTEGER,
      rsuCommRangeFilterValue Integer32,
      rsuCommRange1Min        Integer32,
      rsuCommRange5Min        Integer32,
      rsuCommRange15Min       Integer32,
      rsuCommRangeAvg1Min     Integer32,
      rsuCommRangeAvg5Min     Integer32,
      rsuCommRangeAvg15Min    Integer32,
      rsuCommRangeStatus      RowStatus    }
```

5.13.6.1 RSU Communications Range Index

```
rsuCommRangeIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
```

 © 2020 AASHTO / ITE / NEMA

```
    DESCRIPTION  "<Definition> RSU Channel Index. This value shall not exceed
        maxRsuCommRange.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.12.6.1.1"
::= { rsuCommRangeEntry 1 }
```

5.13.6.2 RSU Communications Range - Geographic Sector

```
rsuCommRangeSector OBJECT-TYPE
    SYNTAX       Integer32 (1..16)
    UNITS        "sector"
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> The geographic sector surrounding the RSU that
        the statistics for this row is for. The geographic area surrounding
        the RSU is divided into sixteen 22.5 degrees sectors. Sector 1 starts
        from North and ends at 22.5 degrees from North in an eastward
        direction.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.12.6.1.2"
::= { rsuCommRangeEntry 2 }
```

5.13.6.3 RSU Communications Range - Message Type

```
rsuCommRangeMsgId OBJECT-TYPE
    SYNTAX       Integer32 (0..32767)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> The SAE J2735 Message Identifier
        (DE_DSRC_MessageID), as defined in SAE J2735, for the message type to
        be reported. A value of '0' means ANY message.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.12.6.1.3"
::= { rsuCommRangeEntry 3 }
```

5.13.6.4 RSU Communications Range - Filter Type

```
rsuCommRangeFilterType OBJECT-TYPE
    SYNTAX       INTEGER {  noFilter(1),
                 vehicleType(2),
                 vehicleClass (3) }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Provides additional filters for the SAE J2735
        messages, such as vehicle type or vehicle class. No filter indicates
        any SAE J2735 message as identified by rsuCommRangeMsgId. vehicleType
        indicates filter by DE_VehicleType as defined in SAE J2735.
        vehicleClass indicates filter by DE_BasicVehicleClass as defined in
        SAE J2735. The value to filter by is defined by
        rsuCommRangeFilterValue.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.12.6.1.4"
::= { rsuCommRangeEntry 4 }
```

5.13.6.5 RSU Communications Range - Filter Value

```
rsuCommRangeFilterValue OBJECT-TYPE
    SYNTAX       Integer32 (0..255)
    MAX-ACCESS   read-create
    STATUS       current
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

```
    DESCRIPTION  "<Definition> The value to filter statistics by, based on
        the filter type defined by rsuCommRangeFilterType. This filter is in
        addition to the SAE J2735 message type, as defined by
        rsuCommRangeMsgId.
        For example, if the value of rsuCommRangeFilterType is vehicleType, a
        value of 4 indicates filter by vehicleType with a value of 4
        (passenger car).
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.12.6.1.5"
::= { rsuCommRangeEntry 5 }
```

5.13.6.6 RSU Communications Range - 1 Minute

```
rsuCommRange1Min OBJECT-TYPE
    SYNTAX       Integer32 (0..2001)
    UNITS        "meter"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> The farthest distance, in meters, from the RSU
        that a message was received via the V2X radio over the previous 1-
        minute period.
        <Valid Value Rule> A value of 0 indicates no messages have been
        received. Values from 1 to 1999 represents 1 meter to 1999 meters. A
        value of 2000 indicates a distance of 2000 meters or greater. A value
        of 2001 indicates unknown.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.12.6.1.6"
::= { rsuCommRangeEntry 6 }
```

5.13.6.7 RSU Communications Range - 5 Minute

```
rsuCommRange5Min OBJECT-TYPE
    SYNTAX       Integer32 (0..2001)
    UNITS        "meter"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> The farthest distance, in meters, from the RSU
        that a message was received via the V2X radio over the previous 5-
        minute period.
        <Valid Value Rule> A value of 0 indicates no messages have been
        received. Values from 1 to 1999 represents 1 meter to 1999 meters. A
        value of 2000 indicates a distance of 2000 meters or greater. A value
        of 2001 indicates unknown.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.12.6.1.7"
::= { rsuCommRangeEntry 7 }
```

5.13.6.8 RSU Communications Range - 15 Minute

```
rsuCommRange15Min OBJECT-TYPE
    SYNTAX       Integer32 (0..2001)
    UNITS        "meter"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> The farthest distance, in meters, from the RSU
        that a message was received via the V2X radio over the previous 15-
        minute period.
        <Valid Value Rule> A value of 0 indicates no messages have been
        received. Values from 1 to 1999 represents 1 meter to 1999 meters. A
```

 © 2020 AASHTO / ITE / NEMA

```
        value of 2000 indicates a distance of 2000 meters or greater. A value
        of 2001 indicates unknown.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.12.6.1.8"
::= { rsuCommRangeEntry 8 }
```

5.13.6.9 RSU Average Communications Range - 1 Minute

```
rsuCommRangeAvg1Min OBJECT-TYPE
    SYNTAX       Integer32 (0..2001)
    UNITS        "meter"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> The average farthest distance, in meters, for
        a mobile device from the RSU that a message was received via the V2X
        radio over the previous 1-minute period.
        <Valid Value Rule> A value of 0 indicates no messages have been
        received. Values from 1 to 1999 represents 1 meter to 1999 meters. A
        value of 2000 indicates a distance of 2000 meters or greater. A value
        of 2001 indicates unknown.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.12.6.1.9"
::= { rsuCommRangeEntry 9 }
```

5.13.6.10 RSU Average Communications Range - 5 Minute

```
rsuCommRangeAvg5Min OBJECT-TYPE
    SYNTAX       Integer32 (0..2001)
    UNITS        "meter"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> The average farthest distance, in meters, for
        a mobile device from the RSU that a message was received via the V2X
        radio over the previous 5-minute period.
        <Valid Value Rule> A value of 0 indicates no messages have been
        received. Values from 1 to 1999 represents 1 meter to 1999 meters. A
        value of 2000 indicates a distance of 2000 meters or greater. A value
        of 2001 indicates unknown.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.12.6.1.10"
::= { rsuCommRangeEntry 10 }
```

5.13.6.11 RSU Average Communications Range - 15 Minute

```
rsuCommRangeAvg15Min OBJECT-TYPE
    SYNTAX       Integer32 (0..2001)
    UNITS        "meter"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> The average farthest distance, in meters, for
        a mobile device from the RSU that a message was received via the V2X
        radio over the previous 15-minute period.
        <Valid Value Rule> A value of 0 indicates no messages have been
        received. Values from 1 to 1999 represents 1 meter to 1999 meters. A
        value of 2000 indicates a distance of 2000 meters or greater. A value
        of 2001 indicates unknown.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.12.6.1.11"
::= { rsuCommRangeEntry 11 }
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

5.13.6.12 RSU Communications Range Status

```
rsuCommRangeStatus OBJECT-TYPE
    SYNTAX       RowStatus
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Create (4) and destroy (6) row entry.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.12.6.1.12"
::= { rsuCommRangeEntry 12 }
```

5.14 System Description

```
rsuSysDescription OBJECT IDENTIFIER ::= { rsu 13 }
```

5.14.1 RSU MIB Version

```
rsuMibVersion OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..32))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Contains the version of this MIB supported by
        this RSU, e.g. rsuMIB 4.1 rev201812060000Z.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.13.1"
::= { rsuSysDescription 1 }
```

5.14.2 RSU Firmware Version

```
rsuFirmwareVersion OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..32))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Contains the version of firmware running on
        this RSU.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.13.2"
::= { rsuSysDescription 2 }
```

5.14.3 RSU Location Description

```
rsuLocationDesc OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..140))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Contains a description of the installation
        location of this RSU.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.13.3"
::= { rsuSysDescription 3 }
```

5.14.4 RSU Identifier

```
rsuID OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..32))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Contains the ID given to this RSU.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.13.4"
::= { rsuSysDescription 4 }
```

 © 2020 AASHTO / ITE / NEMA

5.14.5 RSU Reference Location - Latitude

```
rsuLocationLat OBJECT-TYPE
    SYNTAX       Integer32 (-900000000..900000001)
    UNITS        "tenth of a microdegree"
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Contains the reference latitude of the RSU, in
         10^-7 degrees, using the WGS-84 (World Geodetic System 1984). The
         value 900000001 represents unknown. This value can be used to
         calculate the 2DLocation or 3DLocation field in the IEEE 1609.3 WSA
         header.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.13.5"
    DEFVAL { 900000001 }
::= { rsuSysDescription 5 }
```

5.14.6 RSU Reference Location - Longitude

```
rsuLocationLon OBJECT-TYPE
    SYNTAX       Integer32 (-1800000000..1800000001)
    UNITS        "tenth of a microdegree"
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Contains the reference longitude of the RSU,
         in 10^-7 degrees using the WGS-84 (World Geodetic System 1984). The
         value 1800000001 represents unknown. This value can be used to
         calculate the 2DLocation or 3DLocation field in the IEEE 1609.3 WSA
         header.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.13.6"
    DEFVAL { 1800000001 }
::= { rsuSysDescription 6 }
```

5.14.7 RSU Reference Location - Elevation

```
rsuLocationElv OBJECT-TYPE
    SYNTAX       Integer32 (-100000..1000001)
    UNITS        "centimeter"
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Contains the reference elevation of the RSU,
         as measured to the base of the GNSS antenna, in centimeters above
         the reference ellipsoid as defined by the WGS-84. The value of
         1000001 represents unknown. This value can be used to calculate the
         3DLocation field in the IEEE 1609.3 WSA header.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.13.7"
    DEFVAL { 1000001 }
::= { rsuSysDescription 7 }
```

5.14.8 RSU Reference Location - Elevation Offset

```
rsuElevationOffset OBJECT-TYPE
    SYNTAX       Integer32 (0..2001)
    UNITS        "centimeter"
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION "<Definition> The offset in height, in centimeters, from the
         antenna of a GNSS or similar geopositioning device to the base of
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

```
          the structure that the RSU is mounted on. It is assumed that the
          antenna is at a height higher than the base of the structure.
    <Valid Value Rule> Values of 0 to 2000 provides a range from 0
          centimeters to 2000 centimeters. The value of 2001 represents
          unknown.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.13.8"
    DEFVAL { 2001 }
::= { rsuSysDescription 8 }
```

5.14.9 RSU Installation Command

```
rsuInstallUpdate OBJECT-TYPE
    SYNTAX       INTEGER (0..1)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> This object when set to TRUE (one) shall cause
        the Roadside Unit to begin processing the installation file
        (rsuInstallFile) on the RSU at the scheduled time (See
        rsuScheduledInstallTime). This object shall automatically return to
        FALSE (zero) after the Roadside Unit has issued the update reset
        command. At the successful completion of the installation process,
        the value of the rsuFirmwareVersion object or row in the
        globalModuleTable is also updated.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.13.9"
    DEFVAL { 0 }
::= { rsuSysDescription 9 }
```

5.14.10 RSU Installation Filename

```
rsuInstallFile OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..255))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Represents the name of the installation files
        for the Roadside Unit to process. A SET of the rsuInstallUpdate
        object starts the process to install the referenced file.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.13.10"
::= { rsuSysDescription 10 }
```

5.14.11 RSU Installation Path

```
rsuInstallPath OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(1..255))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Indicates the path where the file to be
         installed (rsuInstallFile) can be found. The path indicated here
         shall be relative to the base directory (see rsuSysDir). The base
         directory is specified by the string '/' (one forward slash). A
         subdirectory from the base may be specified by the string '/subdir'.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.13.11"
::= { rsuSysDescription 11 }
```

 © 2020 AASHTO / ITE / NEMA

5.14.12 RSU Installation Status

```
rsuInstallStatus OBJECT-TYPE
    SYNTAX       INTEGER { other (1),
                 unknown (2),
                 rejected (3),
                 rollbacked (4),
                 processing (5),
                 successful (6) }
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Provides the status of the installation
         process for the RSU. An attempt to update the software may be
         rejected for a security reason, such as it has not been
         authenticated. If applicable, if an attempt to update the software
         fails, the software should be roll-backed to the pre-update version.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.13.12"
::= { rsuSysDescription 12 }
```

5.14.13 RSU Installation Status Time

```
rsuInstallTime OBJECT-TYPE
    SYNTAX       DateAndTime
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Contains the date and time the
         rsuInstallStatus object was last updated. DateAndTime of length 8
         octets.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.13.13"
::= { rsuSysDescription 13 }
```

5.14.14 RSU Installation Status Message

```
rsuInstallStatusMessage OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..255))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> This object conveys a detailed status or error
        message about the status of an installation process. If an attempt to
        update the software fails, this message provides the reason for the
        failure.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.13.14"
::= { rsuSysDescription 14 }
```

5.14.15 RSU Scheduled Installation Time

```
rsuScheduledInstallTime OBJECT-TYPE
    SYNTAX       DateAndTime
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> This object indicates the date and time the
        Roadside Unit is to begin processing the installation file
        (rsuInstallFile) on the RSU. If the value is 00 00 00 00 00 00 00 00,
        then the Roadside Unit shall begin processing the installation file
        as soon as possible. This object shall automatically return to 00 00
        00 00 00 00 00 00 after the Roadside Unit begins processing the
        installation file.
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

```
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.13.15"
::= { rsuSysDescription 15 }
```

5.15 System Settings

```
rsuSysSettings OBJECT IDENTIFIER ::= { rsu 14 }
```

5.15.1 Notification Destination Address

```
rsuNotifyIpAddress OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..64))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Contains the IP address of the SNMP Manager
        that receives the SNMP Notifications (SNMP traps). For an IPv4 remote
        destination, this address can be represented as an IPv4 quad-dotted
        IP address, for example, 192.33.44.235. For IPv6 remote destination,
        this address can be represented as zero-compressed simplified IPv6
        address, for example 2031:0:130F::9C0:876A:130B.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.14.1"
::= { rsuSysSettings 1 }
```

5.15.2 Notification Destination Port

```
rsuNotifyPort OBJECT-TYPE
    SYNTAX       Integer32 (0..65535)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Contains the port number of the SNMP Manager
        that receives the SNMP Notifications (SNMP traps). Default is 162.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.14.2"
    DEFVAL { 162 }
::= { rsuSysSettings 2 }
```

5.15.3 System Log Query Start Time

```
rsuSysLogQueryStart OBJECT-TYPE
    SYNTAX       DateAndTime
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Start time, in UTC, for filtering events. This
        time is supplied in the format of the first 8 octets in the
        DateAndTime field as defined in RFC2579. Example: October 7, 2017 at
        11:34:01.4 PM UTC would be encoded as 07e10a0717220104.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.14.3"
::= { rsuSysSettings 3 }
```

5.15.4 System Log Query Stop Time

```
rsuSysLogQueryStop OBJECT-TYPE
    SYNTAX       DateAndTime
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Stop time, in UTC, for filtering events. This
        time is supplied in the format of the first 8 octets in the
```

 © 2020 AASHTO / ITE / NEMA

```
        DateAndTime field as defined in RFC2579. Example: October 7, 2017 at
        11:34:01.4 PM UTC would be encoded as 07e10a0717220104.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.14.4"
::= { rsuSysSettings 4 }
```

5.15.5 System Log Query Priority

```
rsuSysLogQueryPriority OBJECT-TYPE
    SYNTAX       INTEGER { emergency(0),
                 alert(1),
                 critical(2),
                 error(3),
                 warning(4),
                 notice(5),
                 informational(6),
                 debug(7) }
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> A value as defined below for filtering events
        based on the priority (severity) level as defined in RFC 5424.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.14.5"
    REFERENCE "RFC 5424 Table 2"
::= { rsuSysSettings 5 }
```

5.15.6 System Log Query Generate

```
rsuSysLogQueryGenerate OBJECT-TYPE
    SYNTAX       INTEGER (0..1)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> This object when set to TRUE (one) shall cause
        the RSU to start the creation of a log file for upload using the
        defined filters (e.g., rsuSysLogQueryStart, rsuSysLogQueryStop). This
        object shall automatically return to FALSE (zero) after the RSU has
        issued the start query command and when the log file is available for
        retrieval. The RSU shall also provide the name of the file to be
        retrieved in the rsuSysLogName object.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.14.6"
::= { rsuSysSettings 6 }
```

5.15.7 System Log Query Status

```
rsuSysLogQueryStatus OBJECT-TYPE
    SYNTAX       INTEGER { other (1),
                 unknown (2),
                 progressing (3),
                 successful (4),
                 outOfRange (5),
                 badFilename (6) }
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> The status of an event log query process.
        unknown: The status of unknown or no event log query process in
        progress.
        other: The status of the event log query process is not defined by
        NTCIP 1218.
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

```
        processing: The event log query process is active.
        successful: The event log query process has properly completed.
        outOfRange - The query start or stop time is invalid.
        badFilename - The query filename is invalid.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.14.7"
    DEFVAL { 2 }
::= { rsuSysSettings 7 }
```

5.15.8 System Log Close Command

```
rsuSysLogCloseCommand OBJECT-TYPE
    SYNTAX       INTEGER (0..1)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> This object when set to TRUE (one) shall cause
        the RSU to command the syslog file to close at the earliest
        convenient time. This object shall automatically return to FALSE
        (zero) after the RSU has issued the close command and when the log
        file is available for retrieval. The RSU shall also provide the name
        of the file to be retrieved in the rsuSysLogName object.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.14.8"
::= { rsuSysSettings 8 }
```

5.15.9 System Log Severity

```
rsuSysLogSeverity OBJECT-TYPE
    SYNTAX       SyslogSeverity
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> This object defines the lowest priority level
        of events that are to be recorded in the RSU's syslog. For example, a
        value of error indicates that error conditions are to be logged, in
        addition to critical, alert, and emergency messages. The values are
        defined in RFC 5424.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.14.9"
::= { rsuSysSettings 9 }
```

5.15.10 System Configuration File

```
rsuSysConfigId OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..128))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Contains the name of the system configuration
        to use as part of the RSU's startup functions. The system
        configuration is vendor-specific, but the vendor shall provide and
        document the distinct identifiers that amounts to the system
        configuration parameters.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.14.10"
::= { rsuSysSettings 10 }
```

5.15.11 System Startup Retries

```
rsuSysRetries OBJECT-TYPE
    SYNTAX       Integer32 (0..15)
    MAX-ACCESS   read-write
```

 © 2020 AASHTO / ITE / NEMA

```
    STATUS       current
    DESCRIPTION  "<Definition> This object defines the allowable number of
        attempts within the time defined by the rsuSysRetryPeriod to properly
        reboot an RSU before the RSU enters the 'fault' operating mode. An
        RSU fails to properly reboot if the firmware, operating system, or
        drivers do not load properly during its startup routine as a result
        of a power up or a reboot. A value of 0 indicates this feature is
        disabled (the RSU cannot enter the 'fault' operating mode).
        For example, if the value of this object is 4, the RSU enters the
        'fault' operating mode during a fifth reboot within the
        rsuSysRetryPeriod.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.14.11"
::= { rsuSysSettings 11 }
```

5.15.12 System Startup Retry Period

```
rsuSysRetryPeriod OBJECT-TYPE
    SYNTAX       Integer32 (0..1440)
    UNITS        "minute"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> This object defines the period of time, in
        minutes, during which a user-defined number of startups (See
        rsuSysRetries) are allowed before the RSU enters the 'fault' mode
        operating mode. An RSU fails to properly reboot if the firmware,
        operating system, or drivers do not load properly during its startup
        routine as a result of a power up or a reboot. A value of 0 indicates
        this feature is disabled (the RSU cannot enter the 'fault' operating
        mode).
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.14.12"
::= { rsuSysSettings 12 }
```

5.15.13 Short Communications Loss Time

```
rsuShortCommLossTime OBJECT-TYPE
    SYNTAX       Integer32 (0..65535)
    UNITS        "second"
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Defines the time, in seconds, from the start
        of a communications loss with the management station to the threshold
        where it is considered a short-term communications loss event. A
        value of 0 disables this function. A communications loss is when the
        RSU has not received a valid communications message from the
        management station. A management station may intermittently transmit
        a GET request for any object, such as an object in the
        rsuMsgRepeatStatusTable, to avoid a communication loss event.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.14.13"
    DEFVAL { 0 }
::= { rsuSysSettings 13 }
```

5.15.14 Long Communications Loss Time

```
rsuLongCommLossTime OBJECT-TYPE
    SYNTAX       Integer32 (0..65535)
    UNITS        "minute"
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

```
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Defines the time, in minutes, from the start
        of a communications loss with the management station to the threshold
        where it is considered a long-term communications loss event. A value
        of 0 disables this function. A communications loss is when the RSU
        has not received a valid communications message from the management
        station. A management station may intermittently transmit a GET
        request for any object, such as an object in the
        rsuMsgRepeatStatusTable, to avoid a communication loss event. This
        value should be greater than the value of rsuShortCommLossTime.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.14.14"
    DEFVAL { 0 }
::= { rsuSysSettings 14 }
```

5.15.15 System Log Name

```
rsuSysLogName OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(1..255))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Contains the subdirectory (from the base
         directory - see rsuSysDir) and filename of the file that contains
         the logged events for retrieval. The path indicated here shall be
         relative to the base directory (see rsuSysDir). The base directory
         is specified by the string '/' (one forward slash). A subdirectory
         from the base may be specified by the string '/subdir'.
         For example, if the value of rsuSysDir is '~', and the value of this
         object is '/logs/system.log', the queried log file would be found at
         the path '~/logs/system.log'
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.14.15"
::= { rsuSysSettings 15 }
```

5.15.16 System Base Directory

```
rsuSysDir OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..255))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Contains the base directory from which log
         files may be retrieved from, relative to the home directory (of the
         user account). If no base directory is provided, the default
         directory is '~'. A subdirectory from the home directory may be
         specified by the string '~/subdir'. This value is used by other
         objects to provide the location of files (e.g., log files,
         installation files).
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.14.16"
::= { rsuSysSettings 16 }
```

5.15.17 Long Communications Loss Reboot

```
rsuLongCommLossReboot OBJECT-TYPE
    SYNTAX       INTEGER { disable (0),
                           enable (1) }
    MAX-ACCESS   read-write
    STATUS       current
```

 © 2020 AASHTO / ITE / NEMA

```
    DESCRIPTION  "<Definition> This object when set to TRUE (one) shall cause
         the Roadside Unit to reboot when a long-term communications loss
         event occurs. A value of 0 disables this function (the RSU does not
         reboot). A communications loss is when the RSU has not received a
         valid communications message from the management station. A
         management station may intermittently transmit a GET request for any
         object, such as an object in the rsuMsgRepeatStatusTable, to avoid a
         communication loss event.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.14.17"
    DEFVAL { 0 }
::= { rsuSysSettings 17 }
```

5.15.18 RSU Host Network Address Parameter

```
rsuHostIpAddr OBJECT-TYPE
    SYNTAX      DisplayString (SIZE(0..64))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION "<Definition> Contains the IP address for static IP network
         configuration of the administration ethernet port for this RSU. The
         value of this object is to persist even if power is lost. For an
         IPv4 remote destination, this address can be represented as an IPv4
         quad-dotted IP address, for example, 192.33.44.235. For IPv6 remote
         destination, this address can be represented as zero-compressed
         simplified IPv6 address, for example 2031:0:130F::9C0:876A:130B.
         This object is read-writeable only by a user with administrator
         privileges.
      <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.14.18"
::= { rsuSysSettings 18 }
```

5.15.19 RSU Host Net Mask Parameter

```
rsuHostNetMask OBJECT-TYPE
     SYNTAX      DisplayString (SIZE(0..64))
     MAX-ACCESS  read-write
     STATUS      current
     DESCRIPTION "<Definition> Contains the network mask for static IP
         network configuration of the administration ethernet port for this
         RSU. The value of this object is to persist even if power is lost.
         For an IPv4 remote destination, this address can be represented as
         an IPv4 quad-dotted IP address, for example, 192.33.44.235. For IPv6
         remote destination, this address can be represented as zero-
         compressed simplified IPv6 address, for example
         2031:0:130F::9C0:876A:130B. This object is read-writeable only by a
         user with administrator privileges.
      <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.14.19"
::= { rsuSysSettings 19 }
```

5.15.20 RSU Host Gateway Parameter

```
rsuHostGateway OBJECT-TYPE
     SYNTAX      DisplayString (SIZE(0..64))
     MAX-ACCESS  read-write
     STATUS      current
     DESCRIPTION "<Definition> Contains the gateway IP address for static IP
         network configuration of the administration ethernet port for this
```

© 2020 AASHTO / ITE / NEMA

```
        RSU. The value of this object is to persist even if power is lost.
        For an IPv4 remote destination, this address can be represented as
        an IPv4 quad-dotted IP address, for example, 192.33.44.235. For IPv6
        remote destination, this address can be represented as zero-
        compressed simplified IPv6 address, for example
        2031:0:130F::9C0:876A:130B. This object is read-writeable only by a
        user with administrator privileges.
      <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.20"
::= { rsuSysSettings 20 }
```

5.15.21 RSU Host Domain Name Server Parameter

```
rsuHostDNS OBJECT-TYPE
     SYNTAX DisplayString (SIZE(0..64))
     MAX-ACCESS read-write
     STATUS current
     DESCRIPTION "<Definition> Contains the domain name server IP address of
         the host for configuring network IPs for this RSU. The value of this
         object is to persist even if power is lost. For an IPv4 remote
         destination, this address can be represented as an IPv4 quad-dotted
         IP address, for example, 192.33.44.235. For IPv6 remote destination,
         this address can be represented as zero-compressed simplified IPv6
         address, for example 2031:0:130F::9C0:876A:130B. If the value of
         rsuHostDNS is 0, then DNS is disabled. This object is readwriteable
         only by a user with administrator privileges.
     <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.21"
::= { rsuSysSettings 21 }
```

5.15.22 RSU Host DHCP Enable Parameter

```
rsuHostDHCPEnable OBJECT-TYPE
    SYNTAX       INTEGER { disable(1),  -- static IP is used
                 enable(2)              -- DHCP is used
                 }
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION "<Definition> The indication of whether the administration
         ethernet port of the RSU uses DHCP or the static IP configuration
         settings contained in rsuHostIpAddr, rsuHostNetMask, and
         rsuHostGateway. The value of this object is to persist even if power
         is lost.
      <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.22"
::= { rsuSysSettings 22 }
```

5.16 Antenna Settings

```
rsuAntenna OBJECT IDENTIFIER ::= { rsu 15 }
```

5.16.1 Maximum Antennas

```
maxRsuAntennas OBJECT-TYPE
    SYNTAX       Integer32 (1..64)
    UNITS        "antenna"
    MAX-ACCESS   read-only
    STATUS       current
```

 © 2020 AASHTO / ITE / NEMA

```
    DESCRIPTION "<Definition> The maximum number of V2X antennas this
         Roadside Unit supports. This object indicates the maximum rows which
         appears in the rsuAntennaTable object.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.15.1"
::= { rsuAntenna 1 }
```

5.16.2 Antenna Table

```
rsuAntennaTable OBJECT-TYPE
    SYNTAX       SEQUENCE OF RsuAntennaEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> A table containing V2X antenna parameters. The
         number of rows in this table is equal to the maxRsuAntennas object.
    <TableType> static
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.15.2"
::= { rsuAntenna 2 }

rsuAntennaEntry OBJECT-TYPE
    SYNTAX       RsuAntennaEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "<Definition> Parameters for a specific roadside unit V2X
         antenna.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.15.2.1"
    INDEX { rsuAntennaIndex }
::= { rsuAntennaTable 1 }

RsuAntennaEntry ::= SEQUENCE {
    rsuAntennaIndex   Integer32,
    rsuAntLat         Integer32,
    rsuAntLong        Integer32,
    rsuAntElv         Integer32,
    rsuAntGain        Integer32,
    rsuAntDirection   Integer32 }
```

5.16.2.1 RSU Antenna Index

```
rsuAntennaIndex OBJECT-TYPE
    SYNTAX       Integer32 (1..64)
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "<Definition> Roadside unit V2X antenna Index. This value
         shall not exceed maxRsuAntennas.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.15.2.1.1"
::= { rsuAntennaEntry 1 }
```

5.16.2.2 RSU V2X Antenna - Latitude

```
rsuAntLat OBJECT-TYPE
    SYNTAX       Integer32 (-900000000..900000001)
    UNITS        "tenth of a microdegree"
    MAX-ACCESS   read-write
    STATUS       current
```

© 2020 AASHTO / ITE / NEMA

```
    DESCRIPTION "<Definition> Contains the latitude location, in 10^-7
         degrees, using the WGS-84 (World Geodetic System 1984), of the base
         of the V2X antenna. The value 900000001 represents unknown.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.15.2.1.2"
    DEFVAL { 900000001 }
::= { rsuAntennaEntry 2 }
```

5.16.2.3 RSU V2X Antenna - Longitude

```
rsuAntLong OBJECT-TYPE
    SYNTAX       Integer32 (-1800000000..1800000001)
    UNITS        "tenth of a microdegree"
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION "<Definition> Contains the longitude location, in 10^-7
         degrees, using the WGS-84 (World Geodetic System 1984), of the base
         of the V2X antenna. The value 1800000001 represents unknown.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.15.2.1.3"
    DEFVAL { 1800000001 }
::= { rsuAntennaEntry 3 }
```

5.16.2.4 RSU V2X Antenna - Elevation

```
rsuAntElv OBJECT-TYPE
    SYNTAX       Integer32 (-100000..1000001)
    UNITS        "centimeter"
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION "<Definition> The elevation of the base of the V2X antenna,
         in centimeters above the reference ellipsoid as defined by the WGS-
         84. The value of 1000001 represents unknown.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.15.2.1.4"
    DEFVAL { 1000001 }
::= { rsuAntennaEntry 4 }
```

5.16.2.5 RSU Antenna Gain

```
rsuAntGain OBJECT-TYPE
    SYNTAX       Integer32 (-128..127)
    UNITS        "dB"
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION "<Definition> The antenna gain for the subject antenna in
         hundredths of a dB. The value includes any cable losses.
    <Valid Value Rule> The value of -128 represents unknown.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.15.2.1.5"
::= { rsuAntennaEntry 5 }
```

5.16.2.6 RSU Antenna Directional

```
rsuAntDirection OBJECT-TYPE
    SYNTAX       Integer32 (0..361)
    UNITS        "degree"
    MAX-ACCESS   read-write
    STATUS       current
```

 © 2020 AASHTO / ITE / NEMA

```
    DESCRIPTION "<Definition> The direction that the antenna is pointing (for
         the highest gain), in degrees from true North to the east. A value
         of 90 indicates the antenna is pointing east. A value of 360
         indicates uniform gain in the horizontal plane. A value of 361
         indicates unknown.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.15.2.1.6"
    DEFVAL { 361 }
::= { rsuAntennaEntry 6 }
```

5.17 RSU System Status

```
rsuSystemStatus OBJECT IDENTIFIER ::= { rsu 16 }
```

5.17.1 RSU Radio Status

```
rsuChanStatus OBJECT-TYPE
    SYNTAX       INTEGER {  bothOp (0), --both Continuous and Alternating
                            modes are operational
        altOp (1),   -- Alternating mode is operational, Continuous mode is
                        not operational
        contOp (2),  -- Continuous mode is operational, Alternating mode is
                        not operational
        noneOp (3) }  -- neither Continuous nor Alternating mode is
                        operational
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Indicates which channel modes are operating.
        Note: Operating means the device is functioning as designed,
        configured, and intended.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.16.1"
::= { rsuSystemStatus 1 }
```

5.17.2 RSU Mode

```
rsuMode OBJECT-TYPE
    SYNTAX       INTEGER {  other(1),
                            standby (2),
                            operate (3) }
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Commands the current mode of operation of the
         RSU and provides capability to transition the device into a new
         mode, e.g. from the operate mode to standby mode, etc. Standby
         indicates the V2X radios are not enabled and interface logging is
         disabled. A SET to a value of 'other' shall return a badValueError.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.16.2"
::= { rsuSystemStatus 2 }
```

5.17.3 RSU Mode Status

```
rsuModeStatus OBJECT-TYPE
    SYNTAX       INTEGER {  other (1),
                            standby (2),
                            operate (3),
                            fault (4) }
    MAX-ACCESS   read-only
```

© 2020 AASHTO / ITE / NEMA

```
    STATUS       current
    DESCRIPTION  "<Definition> The current mode of operation of the RSU.
         Standby indicates the V2X radios are not enabled and interface
         logging is disabled. Fault mode indicates the RSU is not fully
         functional, is not transmitting messages over the V2X interface, but
         allows the RSU to upload and install a new firmware or application
         version.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.16.3"
::= { rsuSystemStatus 3 }
```

5.17.4 RSU Reboot

```
rsuReboot OBJECT-TYPE
    SYNTAX       INTEGER (0..1)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> This object when set to TRUE (one) shall cause
         the RSU to (a warm) reboot. This object shall automatically return
         to FALSE (zero) after the reboot command has been issued.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.16.4"
::= { rsuSystemStatus 4 }
```

5.17.5 RSU Clock Source

```
rsuClockSource OBJECT-TYPE
    SYNTAX       INTEGER {  other (1),
                            crystal (2),
                            gnss (3),
                            ntp (4) }
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Specifies the current primary clock source for
         the RSU.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.16.5"
::= { rsuSystemStatus 5 }
```

5.17.6 RSU Clock Status

```
rsuClockSourceStatus OBJECT-TYPE
    SYNTAX       INTEGER {  other (1),
                            active (2),
                            pendingUpdate (3) }
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Specifies the status of the current primary
         clock source for the RSU.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.16.6"
::= { rsuSystemStatus 6 }
```

5.17.7 RSU Clock Source Timeout

```
rsuClockSourceTimeout OBJECT-TYPE
    SYNTAX       Integer32 (0..3600)
    UNITS        "second"
    MAX-ACCESS   read-write
    STATUS       current
```

 © 2020 AASHTO / ITE / NEMA

```
    DESCRIPTION  "<Definition> Specifies the allowable period, in seconds,
         between valid time data from the primary time source. A value of 0
         disables this function.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.16.7"
::= { rsuSystemStatus 7 }
```

5.17.8 RSU Clock Source Queries

```
rsuClockSourceFailedQuery OBJECT-TYPE
    SYNTAX       Integer32 (0..15)
    UNITS        "second"
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Specifies the allowable number of consecutive
         failed attempts to request valid time data from the primary time
         source. A failed attempt is illustrated by no or an invalid response
         from the time source. A value of 0 disables this function.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.16.8"
::= { rsuSystemStatus 8 }
```

5.17.9 RSU Clock Deviation Tolerance

```
rsuClockDeviationTolerance OBJECT-TYPE
    SYNTAX       Integer32 (0..65535)
    UNITS        "millisecond"
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Specifies the allowable tolerance deviation,
         in milliseconds, between two or more different time sources. A value
         of 0 disables this function.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.16.9"
::= { rsuSystemStatus 9 }
```

5.17.10 RSU System Status

```
rsuStatus OBJECT-TYPE
    SYNTAX       INTEGER {  other (1),
                            okay (2),
                            warning (3),
                            critical (4),
                            unknown (5) }
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> The current overall status of the RSU.
         Okay indicates the RSU is fully operational, with no detected
         service errors (See rsuServiceTable).
         Warning indicates the RSU is operating, but an issue is detected
         which may affect its operation, e.g., wrong configuration. This
         status also indicates at least one RSU service has a status of
         warning (See rsuServiceTable).
         Critical indicates an error that has a significant impact on the RSU
         operation, e.g., time source lost. This status also indicates at
         least one RSU service has a status of critical (See
         rsuServiceTable).
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.16.10"
::= { rsuSystemStatus 10 }
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

5.18 Asynchronous Message

```
-- Asynchronous Messages
rsuAsync OBJECT IDENTIFIER ::= { rsu 17 }
```

5.18.1 Notifications

```
-- Notifications

rsuNotifications OBJECT IDENTIFIER ::= { rsuAsync 1 }
```

5.18.1.1 File Integrity Check Error Message

```
messageFileIntegrityError NOTIFICATION-TYPE
    OBJECTS      { rsuAlertLevel, rsuMsgFileIntegrityMsg }
    STATUS       current
    DESCRIPTION  "<Definition> The SNMP agent should immediately report
         integrity check errors on store-and-forward messages or immediate
         forward messages to the SNMP manager. For example, an integrity
         error may be detected if the message does not contain a valid UPER
         encoded message frame.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.1.1"
::= { rsuNotifications 1 }
```

5.18.1.2 Storage Integrity Error Message

```
rsuSecStorageIntegrityError NOTIFICATION-TYPE
    OBJECTS      { rsuAlertLevel, rsuSecStorageIntegrityMsg }
    STATUS       current
    DESCRIPTION  "<Definition> The SNMP agent should immediately report
         integrity check errors in secure storage to the SNMP manager.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.1.2"
::= { rsuNotifications 2 }
```

5.18.1.3 Authorization Error Message

```
rsuAuthError NOTIFICATION-TYPE
    OBJECTS      { rsuAlertLevel, rsuAuthMsg }
    STATUS       current
    DESCRIPTION  "<Definition> The SNMP agent should report an error in
         authorization to the SNMP manager, e.g., attempt to access SNMP
         manager using invalid security credentials.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.1.3"
::= { rsuNotifications 3 }
```

5.18.1.4 Signature Verification Error Message

```
rsuSignatureVerifyError NOTIFICATION-TYPE
    OBJECTS      { rsuAlertLevel, rsuSignatureVerifyMsg }
    STATUS       current
    DESCRIPTION  "<Definition> The SNMP agent should report any signature
         verification errors in received WAVE messages to the SNMP manager.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.1.4"
::= { rsuNotifications 4 }
```

Copy Per MIB Distribution Permission © 2020 AASHTO / ITE / NEMA

5.18.1.5 Access Error Message

```
rsuAccessError NOTIFICATION-TYPE
    OBJECTS      { rsuAlertLevel, rsuAccessMsg }
    STATUS       current
    DESCRIPTION  "<Definition> The SNMP agent should report an access error
         or rejection due to a violation of the Access Control List.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.1.5"
::= { rsuNotifications 5 }
```

5.18.1.6 Time Source Lost Message

```
rsuTimeSourceLost NOTIFICATION-TYPE
    OBJECTS      { rsuAlertLevel, rsuTimeSourceLostMsg }
    STATUS       current
    DESCRIPTION  "<Definition> The SNMP agent should report to the SNMP
         manager that a time source was lost.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.1.6"
::= { rsuNotifications 6 }
```

5.18.1.7 Time Source Mismatch Message

```
rsuTimeSourceMismatch NOTIFICATION-TYPE
    OBJECTS      { rsuAlertLevel, rsuTimeSourceMismatchMsg }
    STATUS       current
    DESCRIPTION  "<Definition> The SNMP agent should report to the SNMP
         manager a deviation between two time sources that exceeds a vendor-
         defined threshold.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.1.7"
::= { rsuNotifications 7 }
```

5.18.1.8 GNSS Anomaly Message

```
rsuGnssAnomaly NOTIFICATION-TYPE
    OBJECTS      { rsuAlertLevel, rsuGnssAnomalyMsg }
    STATUS       current
    DESCRIPTION  "<Definition> The SNMP agent should report any anomalous
         GNSS readings to the SNMP manager.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.1.8"
::= { rsuNotifications 8 }
```

5.18.1.9 GNSS Deviation Error Message

```
rsuGnssDeviationError NOTIFICATION-TYPE
    OBJECTS      { rsuAlertLevel, rsuGnssDeviationMsg }
    STATUS       current
    DESCRIPTION  "<Definition> The SNMP agent should report to the SNMP
         manager a deviation in GNSS position that is greater than the
         configured value.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.1.9"
::= { rsuNotifications 9 }
```

5.18.1.10 GNSS NMEA Message

```
rsuGnssNmeaNotify NOTIFICATION-TYPE
    OBJECTS      { rsuAlertLevel, rsuGnssOutputString }
    STATUS       current
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

```
    DESCRIPTION  "<Definition> The SNMP agent should report the NMEA 0183
         string (including the $ starting character and the ending <CR><LF>)
         to the SNMP manager at the configured interval. This object is used
         in conjunction with the Notification Object provided by
         rsuGnssOutputString.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.1.10"
::= { rsuNotifications 10 }
```

5.18.1.11 Certificate Error Message

```
rsuCertificateError NOTIFICATION-TYPE
    OBJECTS      { rsuAlertLevel, rsuCertificateMsg }
    STATUS       current
    DESCRIPTION  "<Definition> The SNMP agent should report to the SNMP
         manager an error with a certificate.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.1.11"
::= { rsuNotifications 11 }
```

5.18.1.12 Denial of Service Error Message

```
rsuServiceDenialError NOTIFICATION-TYPE
    OBJECTS      { rsuAlertLevel, rsuServiceDenialMsg }
    STATUS       current
    DESCRIPTION  "<Definition> The SNMP agent should report to the SNMP
         manager a detection of a denial of service attack.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.1.12"
::= { rsuNotifications 12 }
```

5.18.1.13 Watchdog Error Message

```
rsuWatchdogError NOTIFICATION-TYPE
    OBJECTS      { rsuAlertLevel, rsuWatchdogMsg }
    STATUS       current
    DESCRIPTION  "<Definition> The SNMP agent should report to the SNMP
         manager a watchdog timer error.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.1.13"
::= { rsuNotifications 13 }
```

5.18.1.14 Enclosure Environment Message

```
rsuEnvironError NOTIFICATION-TYPE
    OBJECTS      { rsuAlertLevel, rsuEnvironMsg }
    STATUS       current
    DESCRIPTION  "<Definition> The SNMP agent should report to the SNMP
         manager an environmental error.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.1.14"
::= { rsuNotifications 14 }
```

5.18.2 Notification Objects

```
rsuNotificationObjects OBJECT IDENTIFIER ::= { rsuAsync 2 }
-- Notification Objects
```

5.18.2.1 File Integrity Check Error Details

```
rsuMsgFileIntegrityMsg OBJECT-TYPE
```

 © 2020 AASHTO / ITE / NEMA

```
    SYNTAX       DisplayString (SIZE(0..255))
    MAX-ACCESS   accessible-for-notify
    STATUS       current
    DESCRIPTION  "<Definition> Contains the error message detailing an Active
         Message integrity error.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.2.1"
::= { rsuNotificationObjects 1 }
```

5.18.2.2 Storage Integrity Error Details

```
rsuSecStorageIntegrityMsg OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..255))
    MAX-ACCESS   accessible-for-notify
    STATUS       current
    DESCRIPTION  "<Definition> Contains the error message detailing a secure
         storage integrity error.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.2.2"
::= { rsuNotificationObjects 2 }
```

5.18.2.3 Authorization Error Details

```
rsuAuthMsg OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..255))
    MAX-ACCESS   accessible-for-notify
    STATUS       current
    DESCRIPTION  "<Definition> Contains the error message detailing an
         authorization error.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.2.3"
::= { rsuNotificationObjects 3 }
```

5.18.2.4 Signature Verification Error Details

```
rsuSignatureVerifyMsg OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..255))
    MAX-ACCESS   accessible-for-notify
    STATUS       current
    DESCRIPTION  "<Definition> Contains the error message detailing a
         signature verification Error.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.2.4"
::= { rsuNotificationObjects 4 }
```

5.18.2.5 Access Error Details

```
rsuAccessMsg OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..255))
    MAX-ACCESS   accessible-for-notify
    STATUS       current
    DESCRIPTION  "<Definition> Contains the error message detailing an error
         or rejection due to Access Control List rules.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.2.5"
::= { rsuNotificationObjects 5 }
```

5.18.2.6 Time Source Lost Details

```
rsuTimeSourceLostMsg OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..255))
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

```
    MAX-ACCESS   accessible-for-notify
    STATUS       current
    DESCRIPTION  "<Definition> Contains the error message indicating a time
         source was lost.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.2.6"
::= { rsuNotificationObjects 6 }
```

5.18.2.7 Time Source Mismatch Details

```
rsuTimeSourceMismatchMsg OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..255))
    MAX-ACCESS   accessible-for-notify
    STATUS       current
    DESCRIPTION  "<Definition> Contains the error message detailing a
         deviation between two time sources that exceeds a vendor-defined
         threshold.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.2.7"
::= { rsuNotificationObjects 7 }
```

5.18.2.8 GNSS Anomaly Details

```
rsuGnssAnomalyMsg OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..255))
    MAX-ACCESS   accessible-for-notify
    STATUS       current
    DESCRIPTION  "<Definition> Contains the error message detailing an
         anomaly that was detected in the GNSS signal.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.2.8"
::= { rsuNotificationObjects 8 }
```

5.18.2.9 GNSS Deviation Error Details

```
rsuGnssDeviationMsg OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..255))
    MAX-ACCESS   accessible-for-notify
    STATUS       current
    DESCRIPTION  "<Definition> Contains the error message indicating that the
         reported GNSS position differs from the reference by more than the
         allowed deviation.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.2.9"
::= { rsuNotificationObjects 9 }
```

5.18.2.10 GNSS NMEA Details

```
rsuGnssNmeaNotifyInterval OBJECT-TYPE
    SYNTAX       Integer32 (0..18000)
    UNITS        "second"
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> Sets the repeat interval in seconds for the
         Notification containing the NMEA GPGGA string. Default is 0
         (disabled).
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.2.10"
::= { rsuNotificationObjects 10 }
```

 © 2020 AASHTO / ITE / NEMA

5.18.2.11 Notification Alert Level

```
rsuAlertLevel OBJECT-TYPE
    SYNTAX       INTEGER {  info(0),
                            notice(1),
                            warning(2),
                            error(3),
                            critical(4)  }
    MAX-ACCESS   accessible-for-notify
    STATUS       current
    DESCRIPTION  "<Definition> The level of importance of the notification.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.2.11"
::= { rsuNotificationObjects 11 }
```

5.18.2.12 Certificate Error Details

```
rsuCertificateMsg OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..255))
    MAX-ACCESS   accessible-for-notify
    STATUS       current
    DESCRIPTION  "<Definition> Contains the error message indicating an error
         with certificate on the RSU was detected, such as there are no
         additional certificates available for distribution or the
         certificates are expired.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.2.12"
::= { rsuNotificationObjects 12 }
```

5.18.2.13 Denial of Service Error Details

```
rsuServiceDenialMsg OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..255))
    MAX-ACCESS   accessible-for-notify
    STATUS       current
    DESCRIPTION  "<Definition> Contains the error message indicating a
         potential denial of service attack was detected.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.2.13"
::= { rsuNotificationObjects 13 }
```

5.18.2.14 Watchdog Error Details

```
rsuWatchdogMsg OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..255))
    MAX-ACCESS   accessible-for-notify
    STATUS       current
    DESCRIPTION  "<Definition> Contains the error message indicating a
         watchdog error was detected.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.2.14"
::= { rsuNotificationObjects 14 }
```

5.18.2.15 Environmental Error Details

```
rsuEnvironMsg OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..255))
    MAX-ACCESS   accessible-for-notify
    STATUS       current
```

© 2020 AASHTO / ITE / NEMA

```
    DESCRIPTION  "<Definition> Contains the error message indicating an
         environmental error was detected such as a high internal
         temperature.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.2.15"
::= { rsuNotificationObjects 15 }
```

5.18.3 Notification Repeat Interval

```
rsuNotificationRepeatInterval OBJECT-TYPE
    SYNTAX       Integer32 (0..255)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> The minimum number of seconds to wait before
         retransmitting a NOTIFICATION-TYPE that has not been acknowledged. A
         value of zero (0) indicates an immediate retransmission of the
         notification message.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.3.3"
::= { rsuAsync 3 }
```

5.18.4 Notification Maximum Retransmission Retries

```
rsuNotificationMaxRetries OBJECT-TYPE
    SYNTAX       Integer32 (0..255)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION  "<Definition> The maximum number of times the RSU attempts
         to retransmit a NOTIFICATION-TYPE that has not been acknowledged.
         Note: A value of one indicates that the RSU attempts a maximum of
         two transmissions (one retry).
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.17.3.4"
::= { rsuAsync 4 }
```

5.19 RSU Applications

```
rsuAppConfig OBJECT IDENTIFIER ::= { rsu 18 }
```

5.19.1 Maximum Applications

```
maxRsuApps OBJECT-TYPE
    SYNTAX       Integer32 (1..65535)
    UNITS        "applications"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "<Definition> The maximum number of applications this
         Roadside Unit supports. This object indicates the maximum rows which
         appears in the rsuAppConfigTable object.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.18.1"
::= { rsuAppConfig 1 }
```

5.19.2 RSU Application Configuration Table

```
rsuAppConfigTable  OBJECT-TYPE
   SYNTAX        SEQUENCE OF RsuAppConfigEntry
   MAX-ACCESS    not-accessible
   STATUS        current
```

 © 2020 AASHTO / ITE / NEMA

```
   DESCRIPTION   "<Definition> A table containing application information.
         This table defines the parameters for the applications on this
         device.
   <TableType>   dynamic
   <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.18.2"
::= { rsuAppConfig 2 }

rsuAppConfigEntry  OBJECT-TYPE
   SYNTAX        RsuAppConfigEntry
   MAX-ACCESS    not-accessible
   STATUS        current
   DESCRIPTION   "<Definition> This object defines an entry in the RSU
         application configuration table.
   <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.18.2.1"
   INDEX { rsuAppConfigID }
::= { rsuAppConfigTable 1 }

RsuAppConfigEntry ::= SEQUENCE {
   rsuAppConfigID       RsuTableIndex,
   rsuAppConfigName     DisplayString,
   rsuAppConfigStartup  INTEGER,
   rsuAppConfigState    INTEGER,
   rsuAppConfigStart    INTEGER,
   rsuAppConfigStop     INTEGER }
```

5.19.2.1 Application Configuration ID Parameter

```
rsuAppConfigID  OBJECT-TYPE
   SYNTAX        RsuTableIndex
   MAX-ACCESS    not-accessible
   STATUS        current
   DESCRIPTION   "<Definition> This object contains the row number which is
         used to identify the application associated with this row in the
         rsuAppConfigTable.
   <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.18.2.1.1"
::= { rsuAppConfigEntry 1 }
```

5.19.2.2 Application Configuration Name

```
rsuAppConfigName  OBJECT-TYPE
   SYNTAX        DisplayString (SIZE(1..127))
   MAX-ACCESS    read-only
   STATUS        current
   DESCRIPTION   "<Definition> This object contains the descriptive name of
         the application associated with this row in the application event
         configuration table. The name should also indicate the application
         version number.
   <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.18.2.1.2"
::= { rsuAppConfigEntry 2 }
```

5.19.2.3 Application Configuration Startup Parameter

```
rsuAppConfigStartup  OBJECT-TYPE
   SYNTAX        INTEGER { other (1),
                     onStartup (2),
                     notStartup (3) }
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

```
   MAX-ACCESS    read-write
   STATUS        current
   DESCRIPTION   "<Definition> This object specifies whether the application
         is to be started when the RSU is powered on or rebooted. A SET to a
         value of other(1) shall return a badValue error.
   <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.18.2.1.3"
::= { rsuAppConfigEntry 3 }
```

5.19.2.4 Application Configuration State

```
rsuAppConfigState  OBJECT-TYPE
   SYNTAX        INTEGER { started (0),
                    stopped (1) }
   MAX-ACCESS    read-only
   STATUS        current
   DESCRIPTION   "<Definition> This object specifies whether the application
         is running on the RSU.
   <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.18.2.1.4"
::= { rsuAppConfigEntry 4 }
```

5.19.2.5 Application Configuration Start Command Parameter

```
rsuAppConfigStart  OBJECT-TYPE
   SYNTAX        INTEGER (0..1)
   MAX-ACCESS    read-write
   STATUS        current
   DESCRIPTION   "<Definition> This object when set to TRUE (one) shall cause
         the RSU to command the application to start at the earliest
         convenient time. This object shall automatically return to FALSE
         (zero) after the RSU has issued the start command.
   <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.18.2.1.5"
::= { rsuAppConfigEntry 5 }
```

5.19.2.6 Application Configuration Stop Command Parameter

```
rsuAppConfigStop  OBJECT-TYPE
   SYNTAX        INTEGER (0..1)
   MAX-ACCESS    read-write
   STATUS        current
   DESCRIPTION   "<Definition> This object when set to TRUE (one) shall cause
         the RSU to command the application to stop at the earliest
         convenient time. This object shall automatically return to FALSE
         (zero) after the RSU has issued the stop command.
   <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.18.2.1.6"
::= { rsuAppConfigEntry 6 }
```

5.20 RSU Services

```
rsuService OBJECT IDENTIFIER ::= { rsu 19 }
```

5.20.1 Maximum RSU Service Entries

```
maxRsuServices OBJECT-TYPE
    SYNTAX       Integer32 (1..65535)
    UNITS        "service"
    MAX-ACCESS   read-only
```

 © 2020 AASHTO / ITE / NEMA

```
    STATUS       current
    DESCRIPTION "<Definition> The maximum number of services this Roadside
         Unit supports. This object indicates the maximum rows which appears
         in the rsuServiceTable object.
    <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.18.19.1"
::= { rsuService 1 }
```

5.20.2 RSU Services Table

```
rsuServiceTable  OBJECT-TYPE
   SYNTAX        SEQUENCE OF RsuServiceEntry
   MAX-ACCESS    not-accessible
   STATUS        current
   DESCRIPTION   "<Definition> A table containing the status of RSU services
         on this device.
   <TableType>   dynamic
   <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.19.2"
::= { rsuService 2 }

rsuServiceEntry  OBJECT-TYPE
   SYNTAX        RsuServiceEntry
   MAX-ACCESS    not-accessible
   STATUS        current
   DESCRIPTION   "<Definition> This object defines an entry in the RSU
         services table.
   <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.19.2.1"
   INDEX { rsuServiceID }
::= { rsuServiceTable 1 }

RsuServiceEntry ::= SEQUENCE {
   rsuServiceID         RsuTableIndex,
   rsuServiceName       DisplayString,
   rsuServiceStatus     INTEGER,
   rsuServiceStatusDesc DisplayString,
   rsuServiceStatusTime DateAndTime }
```

5.20.2.1 Service ID Parameter

```
rsuServiceID  OBJECT-TYPE
   SYNTAX        RsuTableIndex
   MAX-ACCESS    not-accessible
   STATUS        current
   DESCRIPTION   "<Definition> This object contains the row number which is
         used to identify the application associated with this row in the
         rsuServiceTable.
   <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.19.2.1.1"
::= { rsuServiceEntry 1 }
```

5.20.2.2 Service Name

```
rsuServiceName  OBJECT-TYPE
   SYNTAX        DisplayString (SIZE(1..127))
   MAX-ACCESS    read-write
   STATUS        current
   DESCRIPTION   "<Definition> This object contains the descriptive name of
         the service associated with this row in the RSU services table. The
```

© 2020 AASHTO / ITE / NEMA Copy per MIB Distribution Permission

```
         first 16 rows are reserved for standard services defined by this
         standard. All remaining rows may be used for vendor specific
         services. The name and assignments for the standard services are as
         follows:
         rsuServiceID   rsuServiceName   Description
               1        RSU system       system services on the RSU
               2        GNSS             GNSS services
               3        Time source      clock sources
               4        Storage          file and log storage available
               5        Firewall         access control services
               6        Network          network services
               7        Layers 1 and 2   radio access technology
               8        Layers 3 and 4   networking services
               9        Security         security services
               10       SCMS             SCMS services
            11-16       RESERVED         reserved for future services
           17-127       vendor-specific  for vendor-specific services
   <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.19.2.1.2"
::= { rsuServiceEntry 2 }
```

5.20.2.3 Service Status

```
rsuServiceStatus  OBJECT-TYPE
    SYNTAX       INTEGER {  other (1),
                            okay (2),
                            warning (3),
                            critical (4),
                            unknown (5) }
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> The current status of the service for that row
         on the RSU.
         Okay indicates the service is fully operational with no errors.
         Warning indicates the service is operating, but an error is detected
         which may affect its operation, e.g., wrong configuration.
         Critical indicates an error is detected that has a significant
         impact on the RSU operation.
   <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.19.2.1.3"
    DEFVAL { unknown }
::= { rsuServiceEntry 3 }
```

5.20.2.4 Service Status Description

```
rsuServiceStatusDesc  OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..255))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Provides detailed information for the current
         status of the service for that row on the RSU, e.g., the cause for a
         Warning status or Critical status value. The value Okay indicates
         the service is fully operational with no errors.
   <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.19.2.1.4"
::= { rsuServiceEntry 4 }
```

 © 2020 AASHTO / ITE / NEMA

5.20.2.5 Service Status Update TIme

```
rsuServiceStatusTime OBJECT-TYPE
    SYNTAX       DateAndTime
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Provides the date and time that the
         rsuServiceStatus was last updated. DateAndTime is of length 8
         octets.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.19.2.1.5"
::= { rsuServiceEntry 5 }
```

5.21 Transmitted Messages For Forwarding

```
rsuXmitMsgFwding OBJECT IDENTIFIER ::= { rsu 20 }
```

5.21.1 Maximum Number of Transmitted Messages for Forwarding

```
maxXmitMsgFwding OBJECT-TYPE
    SYNTAX       Integer32 (1..255)
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> The maximum number of transmitted message
         types (over the V2X interface), times and destinations for
         forwarding this Roadside Unit supports. This object indicates the
         maximum rows which appears in the rsuXmitMsgFwdingTable object.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.20.1"
::= { rsuXmitMsgFwding 1 }
```

5.21.2 Transmitted Messages for Forwarding Table

```
rsuXmitMsgFwdingTable OBJECT-TYPE
    SYNTAX SEQUENCE OF RsuXmitMsgFwdingEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Contains the PSID of messages transmitted over
         the V2X interface being forwarded to a network host, the IP Address
         and port number of the destination host, as well as other
         configuration parameters as defined.
    <TableType>  dynamic
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.20.2"
::= { rsuXmitMsgFwding 2 }

rsuXmitMsgFwdingEntry OBJECT-TYPE
    SYNTAX       RsuXmitMsgFwdingEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> A row describing the messages transmitted over
         the V2X interface to be forwarded.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.20.2.1"
    INDEX        { rsuXmitMsgFwdingIndex }
    ::= { rsuXmitMsgFwdingTable 1 }

RsuXmitMsgFwdingEntry ::= SEQUENCE {
    rsuXmitMsgFwdingIndex              RsuTableIndex,
    rsuXmitMsgFwdingPsid               RsuPsidTC,
    rsuXmitMsgFwdingDestIpAddr         DisplayString,
```

© 2020 AASHTO / ITE / NEMA

```
    rsuXmitMsgFwdingDestPort           Integer32,
    rsuXmitMsgFwdingProtocol           INTEGER,
    rsuXmitMsgFwdingDeliveryStart      DateAndTime,
    rsuXmitMsgFwdingDeliveryStop       DateAndTime,
    rsuXmitMsgFwdingSecure             INTEGER,
    rsuXmitMsgFwdingStatus             RowStatus }
```

5.21.2.1 Transmitted Messages for Forwarding Index

```
rsuXmitMsgFwdingIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Messages Transmitted for Forwarding Table
         Index. This value shall not exceed maxXmitMsgFwding.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.20.2.1.1"
::= { rsuXmitMsgFwdingEntry 1 }
```

5.21.2.2 Transmitted Messages for Forwarding PSID

```
rsuXmitMsgFwdingPsid OBJECT-TYPE
    SYNTAX       RsuPsidTC
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> The Provider Service Identifier (PSID) of a
         Message Transmitted by the RSU over the V2X Interface to be
         forwarded. The current PSID assignments can be found at
         https://standards.ieee.org/products-
         services/regauth/psid/public.html.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.20.2.1.2"
::= { rsuXmitMsgFwdingEntry 2 }
```

5.21.2.3 Transmitted Messages for Forwarding Destination Address

```
rsuXmitMsgFwdingDestIpAddr OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..64))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Destination Server IP address to forward the
         message transmitted by the RSU over the V2X Interface. For an IPv4
         remote destination, this address can be represented as an IPv4 quad-
         dotted IP address, for example, 192.33.44.235. For IPv6 remote
         destination, this address can be represented as zero-compressed
         simplified IPv6 address, for example 2031:0:130F::9C0:876A:130B.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.20.2.1.3"
::= { rsuXmitMsgFwdingEntry 3 }
```

5.21.2.4 Transmitted Messages for Forwarding Destination Port

```
rsuXmitMsgFwdingDestPort OBJECT-TYPE
    SYNTAX       Integer32 (1024..65535)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Destination Server Port Number to forward the
         message transmitted by the RSU over the V2X Interface.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.20.2.1.4"
```

 © 2020 AASHTO / ITE / NEMA

```
::= { rsuXmitMsgFwdingEntry 4 }
```

5.21.2.5 Transmitted Messages for Forwarding Destination Protocol

```
rsuXmitMsgFwdingProtocol OBJECT-TYPE
    SYNTAX       INTEGER { other (1), udp (2) }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Transport Protocol between RSU and Server to
         forward the message transmitted by the RSU over the V2X Interface.

         A SET to a value of 'other' shall return a badValue error.

         NOTE: If other is selected, this object allows for future
         extensions, possibly tcp.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.20.2.1.5"
    DEFVAL { udp }
::= { rsuXmitMsgFwdingEntry 5 }
```

5.21.2.6 Transmitted Messages for Forwarding Start Time

```
rsuXmitMsgFwdingDeliveryStart OBJECT-TYPE
    SYNTAX       DateAndTime
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Start time for RSU to start forwarding
         messages to the network destination in UTC. DateAndTime is of length
         8 octets.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.20.2.1.6"
::= { rsuXmitMsgFwdingEntry 6 }
```

5.21.2.7 Transmitted Messages for Forwarding Stop Time

```
rsuXmitMsgFwdingDeliveryStop OBJECT-TYPE
    SYNTAX       DateAndTime
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Stop time for RSU to stop forwarding messages
         to the network destination in UTC. DateAndTime is of length 8
         octets.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.20.2.1.7"
::= { rsuXmitMsgFwdingEntry 7 }
```

5.21.2.8 Received Message Forward Secure Option

```
rsuXmitMsgFwdingSecure OBJECT-TYPE
    SYNTAX       INTEGER (0..1)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> A value of 0 indicates the RSU is to forward
         only the WSM message payload without security headers. Specifically
         this means that either of the following is forwarded, depending on
         whether the message is signed (a) or unsigned (b): (a)
         Ieee1609Dot2Data.signedData.tbsData.payload.data.unsecuredData or
         (b) Ieee1609Dot2Data.unsecuredData.
```

© 2020 AASHTO / ITE / NEMA

```
          A value of 1 indicates the RSU is to forward the entire WSM
          including the security headers. Specifically this means that the
          entire Ieee1609Dot2Data frame is forwarded in COER format.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.20.2.1.8"
::= { rsuXmitMsgFwdingEntry 8 }
```

5.21.2.9 Transmitted Messages for Forwarding Status

```
rsuXmitMsgFwdingStatus OBJECT-TYPE
    SYNTAX       RowStatus
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Create (4) and destroy (6) row entry.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.20.2.1.9"
::= { rsuXmitMsgFwdingEntry 9 }

END
```

 © 2020 AASHTO / ITE / NEMA

Annex A
Requirements Traceability Matrix (RTM) [Normative]

The Requirements Traceability Matrix (RTM) links the Functional Requirements as presented in Section 3 with the corresponding Dialogs (Section 4.2) on the same (gray) line. Each Functional Requirement/Dialog relates/uses one or more groups of Objects. The Objects (also known as Data Elements) are listed to the side; the formal definition of each object is contained within Section 5. Using this table, each Functional Requirement can thus be traced in a standardized way.

> Note: The INDEX objects into any of the tables are not explicitly exchanged but are used as index values for other objects that are exchanged.

The audience for this table is implementers (manufacturers and central system developers) and conformance testers. Additionally, other interested parties might use this table to determine how particular functions are to be implemented using the standardized dialogs, interfaces, and object definitions.

To conform to a requirement, an RSU system shall implement all objects traced from that requirement; and unless otherwise indicated, shall implement all dialogs traced from the requirement. To be consistent with a requirement, an RSU system shall be able to fulfill the requirement using only objects that a conforming RSU system is required to support.

Section 3 defines Supplemental Requirements, which are refining other functional requirements. These functional requirements in turn are generally traced to design elements (e.g., rather than being directly traced to design elements).

> Note: Visit www.ntcip.org for information on availability of electronic copies of the RTM.

A.1 Notation [Informative]

A.1.1 Functional Requirement Columns

The functional requirements are defined within Section 3 and the RTM is based upon the requirements within that Section. The section number and the functional requirement name are indicated within these columns.

A.1.2 Dialog Column

The standardized dialogs are defined within Section 4 and the RTM references the traces from requirements to this dialog. The section number of the dialog is indicated within this column.

© 2020 AASHTO / ITE / NEMA Copy per RTM Distribution Permission

A.1.3 Object Columns

The objects are defined within Section 5 of NTCIP 1218 v01 or a normative reference (See Section 1.2.1). The RTM references the data objects that are referenced by the dialog. The section number and object name are indicated within these columns.

A.1.4 Additional Specifications

The "Additional Specifications" column may (and should) be used to provide additional notes and requirements about the dialog or may be used by an implementer to provide any additional details about the implementation.

A.2 Instructions For Completing The RTM [Informative]

To find the standardized design content for a functional requirement, search for the requirement identification number and functional requirement under the functional requirements columns. Next to the functional requirements column is a dialog identification number, identifying either a generic dialog (found in Section G.3) or a specified dialog (found in Section 4.2) to be used to fulfill that requirement. To the right of the dialog identification number are the identification number and name of the data objects that are referenced or used by the dialog to fulfill the functional requirement. Object definitions specific to NTCIP 1218 v01 can be found in Section 5. If an object is defined in a different standard, that standard shall be listed first, followed by the section number where the object definition can be found. The "Additional Specifications" column provides additional notes or details about the design content.

A.3 Requirements Traceability Matrix (RTM) Table

Table 8 Requirements Traceability Matrix (RTM)

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
3.4	Architectural Requirements				
3.4.1	Support Basic Communications Requirements				
3.4.1.1	Retrieve Data	G.1			
3.4.1.2	Deliver Data	G.3			
3.4.1.3	Explore Data	G.2			
3.4.2	Log Data Local Storage and Retrieval Requirements				
3.4.2.1	Configure Priority Level for Events	G.3			
			5.15.9	rsuSysLogSeverity	

© 2020 AASHTO / ITE / NEMA

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
3.4.2.2	Close an Active Event Log File	G.3			
			5.15.8	rsuSysLogCloseCommand	
3.4.2.3	Retrieve Event Logged Data	4.2.7			
			5.15.3	rsuSysLogQueryStart	
			5.15.4	rsuSysLogQueryStop	
			5.15.5	rsuSysLogQueryPriority	
			5.15.6	rsuSysLogQueryGenerate	
			5.15.7	rsuSysLogQueryStatus	
			5.15.15	rsuSysLogName	
			5.15.16	rsuSysDir	
3.4.3	Condition-based Exception Reporting	G.6			
3.5	Data Exchange and Operational Environment Requirements				
3.5.1	RSU Configuration Management Requirements				
3.5.1.1	RSU Device Management Requirements				
3.5.1.1.1	Retrieve RSU Identity Requirements				
3.5.1.1.1.1	Store RSU Identifier	G.3			
			5.14.4	rsuID	
3.5.1.1.1.2	Report RSU Component Information	4.2.1			
			1201v03 - 2.2.2	globalMaxModules	
			1201v03 - 2.2.3	globalModuleTable	
			1201v03 - 2.2.3.1	moduleNumber	
			1201v03 - 2.2.3.2	moduleDeviceNode	
			1201v03 - 2.2.3.3	moduleMake	
			1201v03 - 2.2.3.4	moduleModel	

© 2020 AASHTO / ITE / NEMA Copy per RTM Distribution Permission

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			1201v03 - 2.2.3.5	moduleVersion	
			1201v03 - 2.2.3.6	moduleType	
3.5.1.1.1.3	Report Supported Standards	G.1			
			1201v03 - 2.2.4	controllerBaseStandards	
3.5.1.1.1.4	Report RSU System Name	G.1			
			RFC 3418	sysName	
3.5.1.1.1.5	Report RSU MIB Version	G.1			
			5.14.1	rsuMibVersion	
3.5.1.1.2	Report Deployment Configuration Identifier	G.1			
			1201v03 - 2.2.1	globalSetIDParameter	
3.5.1.1.3	Manage RSU Location Requirements				
3.5.1.1.3.1	Store RSU Location Description	G.3			
			5.14.3	rsuLocationDesc	
3.5.1.1.3.2	Store RSU Location	G.3			
			5.14.5	rsuLocationLat	
			5.14.6	rsuLocationLon	
			5.14.7	rsuLocationElv	
3.5.1.1.3.3	Store RSU Location - GNSS Antenna Offset	G.3			Assumes only 1 GNSS antenna.
			5.14.8	rsuElevationOffset	
3.5.1.1.3.4	Store V2X Antenna Offsets	4.2.3			
			5.16.2	rsuAntennaTable	
			5.16.2.1	rsuAntennaIndex	
			5.16.2.2	rsuAntLat	
			5.16.2.3	rsuAntLong	
			5.16.2.4	rsuAntElv	
3.5.1.1.3.5	Report Positioning Augmentation	G.1			

Copy per RTM Distribution Permission © 2020 AASHTO / ITE / NEMA

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			5.3.2	rsuGnssAugmentation	
3.5.1.1.3.6	Forward GNSS Data Requirements				
3.5.1.1.3.6.1	Store GNSS Data Output Destination	G.3			
			5.7.1	rsuGnssOutputPort	
			5.7.2	rsuGnssOutputAddress	
			5.7.3	rsuGnssOutputInterface	
3.5.1.1.3.6.2	Report GNSS Data Output	G.1			
			5.7.5	rsuGnssOutputString	
3.5.1.1.3.6.3	Store GNSS Data Output Interval	G.3			
			5.7.4	rsuGnssOutputInterval	
3.5.1.1.4	Manage RSU Startup Function Requirements				
3.5.1.1.4.1	Determine Maximum Number of Applications Supported	G.1			
			5.19.1	maxRsuApps	
3.5.1.1.4.2	Manage RSU Startup Functions - Applications	4.2.3			
			5.19.2	rsuAppConfigTable	
			5.19.2.1	rsuAppConfigID	
			5.19.2.2	rsuAppConfigName	
			5.19.2.3	rsuAppConfigStartup	
3.5.1.1.4.3	Manage RSU Startup Functions - Configuration File	G.3			

© 2020 AASHTO / ITE / NEMA Copy per RTM Distribution Permission

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			5.15.10	rsuSysConfigId	The system configuration is vendor-specific, but the vendor shall provide the distinct identifiers that comprise the system configuration files. The vendor also shall document how to map those identifiers to the configuration identifier specified by this object.
3.5.1.1.4.4	Configure Startup Retries	G.3			
			5.15.11	rsuSysRetries	
3.5.1.1.4.5	Retrieve Startup Retry Period	G.3			
			5.15.12	rsuSysRetryPeriod	
3.5.1.1.5	Manage RSU Firmware Version Requirements				
3.5.1.1.5.1	Report the RSU Firmware Version	G.1			
			5.14.2	rsuFirmwareVersion	
3.5.1.1.5.2	Update the RSU Firmware Version	4.2.6			
			5.14.9	rsuInstallUpdate	
			5.14.10	rsuInstallFile	
			5.14.11	rsuInstallPath	
			5.14.12	rsuInstallStatus	
			5.14.2	rsuFirmwareVersion	
			5.15.16	rsuSysDir	
3.5.1.1.5.3	Report Firmware Update Status	G.1			
			5.14.12	rsuInstallStatus	
			5.14.13	rsuInstallTime	
			5.14.14	rsuInstallStatusMessage	
3.5.1.1.6	Manage Communications Lost Requirements				
3.5.1.1.6.1	Configure Short-Term Communications Loss	G.3			

Copy per RTM Distribution Permission
© 2020 AASHTO / ITE / NEMA

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			5.15.13	rsuShortCommLossTime	
3.5.1.1.6.2	Configure Long-Term Communications Loss	G.3			
			5.15.14	rsuLongCommLossTime	
3.5.1.1.6.3	Configure Short-Term Communications Event for Stored Messages	4.2.3			
			5.4.2	rsuMsgRepeatStatusTable	
			5.4.2.1	rsuMsgRepeatIndex	
			5.4.2.11	rsuMsgRepeatOptions	
3.5.1.1.6.4	Configure Long-Term Communications Event for Stored Messages	4.2.3			
			5.4.2	rsuMsgRepeatStatusTable	
			5.4.2.1	rsuMsgRepeatIndex	
			5.4.2.11	rsuMsgRepeatOptions	
3.5.1.1.6.5	Configure Short-Term Communications Event for Immediate Forward Messages	4.2.3			
			5.5.2	rsuIFMStatusTable	
			5.5.2.1	rsuIFMIndex	
			5.5.2.7	rsuIFMOptions	
3.5.1.1.6.6	Configure Long-Term Communications Event for Immediate Forward Messages	4.2.3			
			5.5.2	rsuIFMStatusTable	
			5.5.2.1	rsuIFMIndex	
			5.5.2.7	rsuIFMOptions	
3.5.1.1.6.7	Configure Long-Term Communications Event for Reboot	G.3			
			5.15.17	rsuLongCommLossReboot	
3.5.1.1.7	Manage Notification Requirements				
3.5.1.1.7.1	Store Notification Destination Address	G.3			
			5.15.1	rsuNotifyIpAddress	
3.5.1.1.7.2	Store Notification Destination Port	G.3			

© 2020 AASHTO / ITE / NEMA Copy per RTM Distribution Permission

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			5.15.2	rsuNotifyPort	
3.5.1.1.7.3	Notification Message Requirements				
3.5.1.1.7.3.1	Notification - Integrity Check Error - Active Message	G.6			
			5.18.1.1	messageFileIntegrityError	
			5.18.2.1	rsuMsgFileIntegrityMsg	
			5.18.2.11	rsuAlertLevel	
3.5.1.1.7.3.2	Notification - Integrity Check Error - Secure Storage	G.6			
			5.18.1.2	rsuSecStorageIntegrityError	
			5.18.2.2	rsuSecStorageIntegrityMsg	
			5.18.2.11	rsuAlertLevel	
3.5.1.1.7.3.3	Notification - Authorization Verification Error	G.6			
			5.18.1.3	rsuAuthError	
			5.18.2.3	rsuAuthMsg	
			5.18.2.11	rsuAlertLevel	
3.5.1.1.7.3.4	Notification - Signature Verification Error	G.6			
			5.18.1.4	rsuSignatureVerifyError	
			5.18.2.4	rsuSignatureVerifyMsg	
			5.18.2.11	rsuAlertLevel	
3.5.1.1.7.3.5	Notification - Network Access Control List	G.6			
			5.18.1.5	rsuAccessError	
			5.18.2.5	rsuAccessMsg	
			5.18.2.11	rsuAlertLevel	
3.5.1.1.7.3.6	Notification - Time Source Loss	G.6			
			5.18.1.6	rsuTimeSourceList	
			5.18.2.6	rsuTimeSourceLostMsg	
			5.18.2.11	rsuAlertLevel	
3.5.1.1.7.3.7	Notification - Time Source Mismatch	G.6			

Copy per RTM Distribution Permission © 2020 AASHTO / ITE / NEMA

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			5.18.1.7	rsuTimeSourceMismatch	
			5.18.2.7	rsuTimeSourceMismatchMsg	
			5.18.2.11	rsuAlertLevel	
3.5.1.1.7.3.8	Notification - GNSS Anomaly	G.6			
			5.18.1.8	rsuGnssAnomaly	
			5.18.2.8	rsuGnssAnomalyMsg	
			5.18.2.11	rsuAlertLevel	
3.5.1.1.7.3.9	Notification - GNSS Location Deviation	G.6			
			5.18.1.9	rsuGnssDeviationError	
			5.18.2.9	rsuGnssDeviationMsg	
			5.18.2.11	rsuAlertLevel	
3.5.1.1.7.3.10	Notification - Certificate Management	G.6			
			5.18.1.11	rsuCertificateError	
			5.18.2.12	rsuCertificateMsg	
			5.18.2.11	rsuAlertLevel	
3.5.1.1.7.3.11	Notification - Denial of Service	G.6			
			5.18.1.12	rsuServiceDenialError	
			5.18.2.13	rsuServiceDenialMsg	
			5.18.2.11	rsuAlertLevel	
3.5.1.1.7.3.12	Notification - Watchdog	G.6			
			5.18.1.13	rsuWatchdogError	
			5.18.2.14	rsuWatchdogMsg	
			5.18.2.11	rsuAlertLevel	
3.5.1.1.7.3.13	Notification - GNSS Data	G.6			
			5.18.1.10	rsuGnssNmeaNotify	
			5.7.5	rsuGnssOutputString	
			5.18.2.11	rsuAlertLevel	
3.5.1.1.7.3.14	Notification - Configure GNSS Data Interval	G.6			

© 2020 AASHTO / ITE / NEMA Copy per RTM Distribution Permission

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			5.18.2.10	rsuGnssNmeaNotifyInterval	
3.5.1.1.7.3.15	Notification - Environmental	G.6			
			5.18.1.14	rsuEnvironError	
			5.18.2.15	rsuEnvironMsg	
			5.18.2.11	rsuAlertLevel	
3.5.1.1.7.3.16	Notification - Authentication Failure	G.6			
			RFC 3418	authenticationFailure	
3.5.1.1.7.4	Store Notification Type	4.2.4			
			RFC 3413	snmpNotifyTable	SNMP-Notification-MIB
			RFC 3413	snmpNotifyEntry	
			RFC 3413	snmpNotifyName	
			RFC 3413	snmpNotifyTag	
			RFC 3413	snmpNotifyType	
			RFC 3413	snmpNotifyStorageType	
			RFC 3413	snmpNotifyRowStatus	
3.5.1.1.7.5	Store Notification Repeat Intervals	G.3			
			5.18.3	rsuNotificationRepeatInterval	
3.5.1.1.7.6	Store Notification Retries	G.3			
			5.18.4	rsuNotificationMaxRetries	
3.5.1.2	Manage Network Interface Requirements				
3.5.1.2.1	Manage a Network Interface Requirements				
3.5.1.2.1.1	Enable/Disable a Communications Port	4.2.3			
			2103v02 - A.4.3.4 if.2.1	ifIndex	
			2103v02 - A.4.3.4 if.2.3	ifType	

Copy per RTM Distribution Permission
© 2020 AASHTO / ITE / NEMA

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			2103v02 - A.4.3.4 if.2.7	ifAdminStatus	
			2103v02 - A.4.3.4 if.2.8	ifOperStatus	
3.5.1.2.1.2	Configure Ethernet Ports	G.3			
			5.15.18	rsuHostIpAddr	
			5.15.19	rsuHostNetMask	
			5.15.20	rsuHostGateway	
			5.15.21	rsuHostDNS	
			5.15.22	rsuHostDHCPEnable	
3.5.1.2.1.3	Report Ethernet Port - MAC Address	4.2.2			
			2103v02 - A.4.3.4 if.2	ifTable	
			2103v02 - A.4.3.4 if.2.1	ifIndex	
			2103v02 - A.4.3.4 if.2.6	ifPhysAddress	
3.5.1.2.2	Message Management Requirements				
3.5.1.2.2.1	Manage Stored Message Requirements				
3.5.1.2.2.1.1	Determine Maximum Number of Stored Messages Supported	G.1			
			5.4.1	maxRsuMsgRepeat	
3.5.1.2.2.1.2	Store a Message	4.2.3			
			5.4.2	rsuMsgRepeatStatusTable	
			5.4.2.1	rsuMsgRepeatIndex	
			5.4.2.2	rsuMsgRepeatPsid	

© 2020 AASHTO / ITE / NEMA Copy per RTM Distribution Permission

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			5.4.2.3	rsuMsgRepeatTxChannel	
			5.4.2.4	rsuMsgRepeatTxInterval	
			5.4.2.7	rsuMsgRepeatPayload	
			5.4.2.9	rsuMsgRepeatStatus	
3.5.1.2.2.1.3	Delete a Stored Message	4.2.3			
			5.4.2	rsuMsgRepeatStatusTable	
			5.4.2.1	rsuMsgRepeatIndex	
			5.4.2.9	rsuMsgRepeatStatus	
3.5.1.2.2.1.4	Enable/Disable the Transmission of a Stored Message	4.2.3			
			5.4.2	rsuMsgRepeatStatusTable	
			5.4.2.1	rsuMsgRepeatIndex	
			5.4.2.8	rsuMsgRepeatEnable	
3.5.1.2.2.1.5	Store a Message Type	4.2.3			
			5.4.2	rsuMsgRepeatStatusTable	
			5.4.2.1	rsuMsgRepeatIndex	
			5.4.2.7	rsuMsgRepeatPayload	
3.5.1.2.2.1.6	Store PSID for Application Data Exchanges	4.2.3			
			5.4.2	rsuMsgRepeatStatusTable	
			5.4.2.1	rsuMsgRepeatIndex	
			5.4.2.2	rsuMsgRepeatPsid	
3.5.1.2.2.1.7	Delete All Stored Messages	G.3			
			5.4.3	rsuMsgRepeatDeleteAll	
3.5.1.2.2.1.8	Store a Message's Priority	4.2.3			
			5.4.2	rsuMsgRepeatStatusTable	
			5.4.2.1	rsuMsgRepeatIndex	
			5.4.2.10	rsuMsgRepeatPriority	
3.5.1.2.2.1.9	Store a Message's Transmission Interval	4.2.3			
			5.4.2	rsuMsgRepeatStatusTable	

Copy per RTM Distribution Permission © 2020 AASHTO / ITE / NEMA

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			5.4.2.1	rsuMsgRepeatIndex	
			5.4.2.4	rsuMsgRepeatTxInterval	
3.5.1.2.2.1.10	Store a Message's Transmission Channel	4.2.3			
			5.4.2	rsuMsgRepeatStatusTable	
			5.4.2.1	rsuMsgRepeatIndex	
			5.4.2.3	rsuMsgRepeatTxChannel	
3.5.1.2.2.1.11	Store a Message's Transmission Start Time	4.2.3			
			5.4.2	rsuMsgRepeatStatusTable	
			5.4.2.1	rsuMsgRepeatIndex	
			5.4.2.5	rsuMsgRepeatDeliveryStart	
3.5.1.2.2.1.12	Store a Message's Transmission Stop Time	4.2.3			
			5.4.2	rsuMsgRepeatStatusTable	
			5.4.2.1	rsuMsgRepeatIndex	
			5.4.2.6	rsuMsgRepeatDeliveryStop	
3.5.1.2.2.1.13	Store if a Message is to be Signed	4.2.3			
			5.4.2	rsuMsgRepeatStatusTable	
			5.4.2.1	rsuMsgRepeatIndex	
			5.4.2.11	rsuMsgRepeatOptions	
3.5.1.2.2.2	Manage Immediate Forward Message Requirements				
3.5.1.2.2.2.1	Determine Maximum Number of Immediate Forward Messages Supported	G.1			
			5.5.1	maxRsuIFMs	
3.5.1.2.2.2.2	Forward Message to the V2X Interface	4.2.3			
			5.5.2	rsuIFMStatusTable	
			5.5.2.1	rsuIFMIndex	
			5.5.2.2	rsuIFMPsid	
			5.5.2.3	rsuIFMTxChannel	
			5.5.2.4	rsuIFMEnable	

© 2020 AASHTO / ITE / NEMA Copy per RTM Distribution Permission

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			5.5.2.5	rsuIFMStatus	
			5.5.2.8	rsuIFMPayload	
3.5.1.2.2.2.3	Store the Message Type for a Message for Forwarding to the V2X Interface	4.2.3			
			5.5.2	rsuIFMStatusTable	
			5.5.2.1	rsuIFMIndex	
			5.5.2.8	rsuIFMPayload	
3.5.1.2.2.2.4	Store the PSID for an Application Data Exchange for Forwarding to the V2X	4.2.3			
			5.5.2	rsuIFMStatusTable	
			5.5.2.1	rsuIFMIndex	
			5.5.2.2	rsuIFMPsid	
3.5.1.2.2.2.5	Store the Priority for a Message for Forwarding to the V2X Interface	4.2.3			
			5.5.2	rsuIFMStatusTable	
			5.5.2.1	rsuIFMIndex	
			5.5.2.6	rsuIFMPriority	
3.5.1.2.2.2.6	Store the Transmission Channel for a Message for Forwarding to the V2X Interface	4.2.3			
			5.5.2	rsuIFMStatusTable	
			5.5.2.1	rsuIFMIndex	
			5.5.2.3	rsuIFMTxChannel	
3.5.1.2.2.2.7	Store if a Received Message for Forwarding to the V2X Interface is Signed	4.2.3			
			5.5.2	rsuIFMStatusTable	
			5.5.2.1	rsuIFMIndex	
			5.5.2.7	rsuIFMOptions	
3.5.1.2.2.3	Manage Messages Received from the V2X Interface Requirements				

Copy per RTM Distribution Permission
© 2020 AASHTO / ITE / NEMA

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
3.5.1.2.2.3.1	Determine Maximum Number of Message Received Types Supported	G.1			
			5.6.1	maxRsuReceivedMsgs	
3.5.1.2.2.3.2	Store Network Destination to Forward Messages Received from the V2X Interface	4.2.3			
			5.6.2	rsuReceivedMsgTable	
			5.6.2.1	rsuReceivedMsgIndex	
			5.6.2.2	rsuReceivedMsgPsid	
			5.6.2.3	rsuReceivedMsgDestIpAddr	
			5.6.2.4	rsuReceivedMsgDestPort	
			5.6.2.10	rsuReceivedMsgStatus	
3.5.1.2.2.3.3	Store Transport Protocol to Forward Messages Received from the V2X Interface	4.2.3			
			5.6.2	rsuReceivedMsgTable	
			5.6.2.1	rsuReceivedMsgIndex	
			5.6.2.2	rsuReceivedMsgPsid	
			5.6.2.5	rsuReceivedMsgProtocol	
3.5.1.2.2.3.4	Store Minimum Signal Strength to Forward Messages Received from the V2X Interface	4.2.3			
			5.6.2	rsuReceivedMsgTable	
			5.6.2.1	rsuReceivedMsgIndex	
			5.6.2.2	rsuReceivedMsgPsid	
			5.6.2.6	rsuReceivedMsgRssi	
3.5.1.2.2.3.5	Store Message Interval to Forward Messages Received from the V2X Interface	4.2.3			
			5.6.2	rsuReceivedMsgTable	
			5.6.2.1	rsuReceivedMsgIndex	
			5.6.2.2	rsuReceivedMsgPsid	
			5.6.2.7	rsuReceivedMsgInterval	

© 2020 AASHTO / ITE / NEMA Copy per RTM Distribution Permission

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
3.5.1.2.2.3.6	Store Start Time to Forward Messages Received from the V2X Interface	4.2.3			
			5.6.2	rsuReceivedMsgTable	
			5.6.2.1	rsuReceivedMsgIndex	
			5.6.2.2	rsuReceivedMsgPsid	
			5.6.2.8	rsuReceivedMsgDeliveryStart	
3.5.1.2.2.3.7	Store Stop Time to Forward Messages Received from the V2X Interface	4.2.3			
			5.6.2	rsuReceivedMsgTable	
			5.6.2.1	rsuReceivedMsgIndex	
			5.6.2.2	rsuReceivedMsgPsid	
			5.6.2.9	rsuReceivedMsgDeliveryStop	
3.5.1.2.2.3.8	Enable/Disable Forwarding Messages Received from the V2X Interface	4.2.3			
			5.6.2	rsuReceivedMsgTable	
			5.6.2.1	rsuReceivedMsgIndex	
			5.6.2.2	rsuReceivedMsgPsid	
			5.6.2.7	rsuReceivedMsgInterval	SET to 0.
3.5.1.2.2.3.9	Store Secure Options to Forward Messages Received from the V2X Interface	4.2.3			
			5.6.2	rsuReceivedMsgTable	
			5.6.2.1	rsuReceivedMsgIndex	
			5.6.2.2	rsuReceivedMsgPsid	
			5.6.2.11	rsuReceivedMsgSecure	
3.5.1.2.2.3.10	Store Interval to Authenticate Messages Received from the V2X Interface	4.2.3			
			5.6.2	rsuReceivedMsgTable	
			5.6.2.1	rsuReceivedMsgIndex	

Copy per RTM Distribution Permission
© 2020 AASHTO / ITE / NEMA

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			5.6.2.2	rsuReceivedMsgPsid	
			5.6.2.12	rsuReceivedMsgAuthMsgInterval	
3.5.1.2.2.4	Forward Messages Transmitted Over the V2X Interface Requirements				
3.5.1.2.2.4.1	Determine Maximum Number of Message Entries Transmitted Over the V2X Interface For Forwarding Supported	G.1			
			5.21.1	maxXmitMsgFwding	
3.5.1.2.2.4.2	Store Network Destination to Forward Messages Transmitted Over the V2X Interface	4.2.3			
			5.21.2	rsuXmitMsgFwdingTable	
			5.21.2.1	rsuXmitMsgFwdingIndex	
			5.21.2.2	rsuXmitMsgFwdingPsid	
			5.21.2.3	rsuXmitMsgFwdingDestIpAddr	
			5.21.2.4	rsuXmitMsgFwdingDestPort	
			5.21.2.8	rsuXmitMsgFwdingSecure	
			5.21.2.9	rsuXmitMsgFwdingStatus	
3.5.1.2.2.4.3	Store Transport Protocol to Forward Messages Transmitted Over the V2X Interface	4.2.3			
			5.21.2	rsuXmitMsgFwdingTable	
			5.21.2.1	rsuXmitMsgFwdingIndex	
			5.21.2.2	rsuXmitMsgFwdingPsid	
			5.21.2.5	rsuXmitMsgFwdingProtocol	
3.5.1.2.2.4.4	Store Start Time to Forward Messages Transmitted Over the V2X Interface	4.2.3			
			5.21.2	rsuXmitMsgFwdingTable	
			5.21.2.1	rsuXmitMsgFwdingIndex	

© 2020 AASHTO / ITE / NEMA Copy per RTM Distribution Permission

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			5.21.2.2	rsuXmitMsgFwdingPsid	
			5.21.2.6	rsuXmitMsgFwdingDeliveryStart	
3.5.1.2.2.4.5	Store Stop Time to Forward Messages Transmitted Over the V2X Interface	4.2.3			
			5.21.2	rsuXmitMsgFwdingTable	
			5.21.2.1	rsuXmitMsgFwdingIndex	
			5.21.2.2	rsuXmitMsgFwdingPsid	
			5.21.2.7	rsuXmitMsgFwdingDeliveryStop	
3.5.1.2.3	Logging of Interface Data Requirements				
3.5.1.2.3.1	Determine Maximum Number of Interface Logs Supported	G.1			
			5.8.1	maxRsuInterfaceLogs	
3.5.1.2.3.2	Log Interface Data Identification	4.2.3			
			5.8.2	rsuInterfaceLogTable	
			5.8.2.1	rsuIfaceLogIndex	
			5.8.2.2	rsuIfaceGenerate	
			5.8.2.6	rsuIfaceName	
			5.8.2.12	rsuIfaceLogStatus	
3.5.1.2.3.3	Log Interface Data by Direction	4.2.3			
			5.8.2	rsuInterfaceLogTable	
			5.8.2.1	rsuIfaceLogIndex	
			5.8.2.5	rsuIfaceLogByDir	
3.5.1.2.3.4	Store Interface Data Log - File Directory	4.2.3			
			5.8.2	rsuInterfaceLogTable	
			5.8.2.1	rsuIfaceLogIndex	
			5.8.2.7	rsuIfaceStoragePath	
3.5.1.2.3.5	Retrieve Interface Logged Data	4.2.5			

Copy per RTM Distribution Permission
© 2020 AASHTO / ITE / NEMA

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			5.8.2	rsuInterfaceLogTable	
			5.8.2.1	rsuIfaceLogIndex	
			5.8.2.7	rsuIfaceStoragePath	
3.5.1.2.3.6	Store an Interface Data Log Start Time	4.2.3			
			5.8.2	rsuInterfaceLogTable	
			5.8.2.1	rsuIfaceLogIndex	
			5.8.2.9	rsuIfaceLogStart	
3.5.1.2.3.7	Store an Interface Data Log Stop Time	4.2.3			
			5.8.2	rsuInterfaceLogTable	
			5.8.2.1	rsuIfaceLogIndex	
			5.8.2.10	rsuIfaceLogStop	
3.5.1.2.3.8	Store Maximum Interface Data Log File Size	4.2.3			
			5.8.2	rsuInterfaceLogTable	
			5.8.2.1	rsuIfaceLogIndex	
			5.8.2.3	rsuIfaceMaxFileSize	
3.5.1.2.3.9	Store Maximum Interface Data Log File Collection Time	4.2.3			
			5.8.2	rsuInterfaceLogTable	
			5.8.2.1	rsuIfaceLogIndex	
			5.8.2.4	rsuIfaceMaxFileTime	
3.5.1.2.3.10	Store Interface Data Log Option - Disk Full	4.2.3			
			5.8.2	rsuInterfaceLogTable	
			5.8.2.1	rsuIfaceLogIndex	
			5.8.2.11	rsuIfaceLogOptions	
3.5.1.2.3.11	Store Interface Data Log Option - Entry Deletion	4.2.3			
			5.8.2	rsuInterfaceLogTable	
			5.8.2.1	rsuIfaceLogIndex	
			5.8.2.11	rsuIfaceLogOptions	

© 2020 AASHTO / ITE / NEMA Copy per RTM Distribution Permission

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
3.5.1.3	Configure V2X Interfaces Requirements				
3.5.1.3.1	Configure Radio Requirements				
3.5.1.3.1.1	Report Maximum Number of V2X Radios Supported	G.1			
			5.2.1	maxRsuRadios	
3.5.1.3.1.2	Report Type of V2X Radio	4.2.1			
			5.2.2	rsuRadioTable	
			5.2.2.1	rsuRadioIndex	
			5.2.2.4	rsuRadioType	
3.5.1.3.1.3	Enable/Disable Radios	4.2.3			
			5.2.2	rsuRadioTable	
			5.2.2.1	rsuRadioIndex	
			5.2.2.3	rsuRadioEnable	
3.5.1.3.1.4	Report Radio MAC Address	4.2.2			
			5.2.2	rsuRadioTable	
			5.2.2.1	rsuRadioIndex	
			5.2.2.5	rsuRadioMacAddress1	
			5.2.2.6	rsuRadioMacAddress2	
3.5.1.3.1.5	Report Radio Operating Modes	G.1			
			5.17.1	rsuChanStatus	
3.5.1.3.2	Determine Lower Layer Requirements				
3.5.1.3.2.1	Determine Lower Layer Parameter	4.2.2			
			IEEE802dot11-MIB	dot11EDCATable	
			IEEE802dot11-MIB	dot11EDCATableIndex	
			IEEE802dot11-MIB	dot11EDCATableCWmin	
			IEEE802dot11-MIB	dot11EDCATableCWmax	

Copy per RTM Distribution Permission
© 2020 AASHTO / ITE / NEMA

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			IEEE802dot11-MIB	dot11EDCATableAIFSN	
3.5.1.3.2.2	Determine Operating Class	4.2.2			
			2103v02 - A.4.3.4 if.2	ifTable	
			2103v02 - A.4.3.4 if.2.1	ifIndex	
			IEEE802dot11-MIB	dot11OperatingClassesTable	
			IEEE802dot11-MIB	dot11OperatingClassesIndex	
			IEEE802dot11-MIB	dot11OperatingClass	If queried, return the behavior limit for the corresponding class for ITS operations.
3.5.1.3.3	Configure IEEE 1609 Communications Requirements				
3.5.1.3.3.1	Manage IEEE 1609.2 Security Requirements				
3.5.1.3.3.1.1	Report IEEE 1609.2 Enrollment Certificate - Status	G.1			
			5.9.2	rsuSecEnrollCertStatus	
3.5.1.3.3.1.2	Report IEEE 1609.2 Enrollment Certificate - Expiration Date	G.1			
			5.9.6	rsuSecEnrollCertExpiration	
3.5.1.3.3.1.3	Report IEEE 1609.2 Enrollment Certificate - Source Domain	G.1			
			5.9.4	rsuSecEnrollCertUrl	
3.5.1.3.3.1.4	Report IEEE 1609.2 Enrollment Certificate Identifier	G.1			
			5.9.5	rsuSecEnrollCertId	

© 2020 AASHTO / ITE / NEMA Copy per RTM Distribution Permission

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
3.5.1.3.3.1.5	Report IEEE 1609.2 Enrollment Certificate - Valid Region	G.1			
			5.9.3	rsuSecEnrollCertValidRegion	
3.5.1.3.3.1.6	Report IEEE 1609.2 Enrollment Certificate - Source	G.1			
			5.9.7	rsuSecuritySource	
3.5.1.3.3.1.7	Report IEEE 1609.2 Application Certificates - Status	4.2.1			
			5.9.9	maxRsuSecAppCerts	
			5.9.10	rsuSecAppCertTable	
			5.9.10.1	rsuSecAppCertIndex	
			5.9.10.2	rsuSecAppCertPsid	
			5.9.10.3	rsuSecAppCertState	
			5.9.10.4	rsuSecAppCertExpiration	
3.5.1.3.3.1.8	Report IEEE 1609.2 Application Certificates - Source	G.1			
			5.9.8	rsuSecAppCertUrl	
3.5.1.3.3.1.9	Store IEEE 1609.2 Application Certificates - Default Request Interval	G.1			
			5.9.1	rsuSecCredReq	
3.5.1.3.3.1.10	Store IEEE 1609.2 Application Certificates - Request Interval	4.2.3			
			5.9.10	rsuSecAppCertTable	
			5.9.10.1	rsuSecAppCertIndex	
			5.9.10.2	rsuSecAppCertPsid	
			5.9.10.5	rsuSecAppCertReq	
3.5.1.3.3.1.11	Report Certificate Revocation List - Source	G.1			
			5.9.11	rsuSecCertRevocationUrl	
3.5.1.3.3.1.12	Report Certificate Revocation List - Update Time	G.1			

Copy per RTM Distribution Permission
© 2020 AASHTO / ITE / NEMA

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			5.9.12	rsuSecCertRevocationTime	
3.5.1.3.3.1.13	Store Certificate Revocation List Update Interval	G.1			
			5.9.13	rsuSecCertRevocationInterval	
3.5.1.3.3.1.14	Update Certificate Revocation List Command	G.1			
			5.9.14	rsuSecCertRevocationUpdate	
3.5.1.3.3.1.15	Report IEEE 1609.2 Security Profiles	4.2.1			
			5.9.15	maxRsuSecProfiles	
			5.9.16	rsuSecProfileTable	
			5.9.16.1	rsuSecProfileIndex	
			5.9.16.2	rsuSecProfileName	
			5.9.16.3	rsuSecProfileDesc	
3.5.1.3.3.2	Configure IEEE 1609.3 Communications - WSA Requirements				
3.5.1.3.3.2.1	Determine Maximum Number of Services Advertised	G.1			
			5.10.1	maxRsuWsaServices	
3.5.1.3.3.2.2	Store WSA Configuration - Service Info Segment	4.2.3			
			5.10.2	rsuWsaServiceTable	
			5.10.2.1	rsuWsaIndex	
			5.10.2.2	rsuWsaPsid	
			5.10.2.3	rsuWsaPriority	
			5.10.2.4	rsuWsaPSC	
			5.10.2.5	rsuWsaIpAddress	
			5.10.2.6	rsuWsaPort	
			5.10.2.7	rsuWsaChannel	
			5.10.2.8	rsuWsaStatus	

© 2020 AASHTO / ITE / NEMA Copy per RTM Distribution Permission

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			5.10.2.9	rsuWsaMacAddress	
			5.10.2.11	rsuWsaRcpiThreshold	
			5.10.2.12	rsuWsaCountThreshold	
			5.10.2.13	rsuWsaCountThresholdInterval	
			5.10.2.14	rsuWsaRepeatRate	
			5.10.2.15	rsuWsaAdvertiserIdentifier	
			5.10.2.16	rsuWsaEnable	
3.5.1.3.3.2.3	Store WSA Configuration - Channel Info Segment	4.2.3			
			5.10.3	rsuWsaChannelTable	
			5.10.3.1	rsuWsaChannelIndex	
			5.10.3.2	rsuWsaChannelPsid	
			5.10.3.3	rsuWsaChannelNumber	
			5.10.3.4	rsuWsaChannelTxPowerLevel	
			5.10.3.5	rsuWsaChannelAccess	
			5.10.3.6	rsuWsaChannelStatus	
3.5.1.3.3.2.4	Configure WSA Configuration - WAVE Router Advertisement	4.2.3			
			5.11.1	rsuWraIpPrefix	
			5.11.2	rsuWraIpPrefixLength	
			5.11.3	rsuWraGateway	
			5.11.4	rsuWraPrimaryDns	
			5.11.5	rsuWraSecondaryDns	
			5.11.6	rsuWraGatewayMacAddress	
			5.11.7	rsuWraLifetime	
3.5.1.3.3.2.5	Store WSA Configuration - Secure	4.2.3			
			5.10.2	rsuWsaServiceTable	

Copy per RTM Distribution Permission
© 2020 AASHTO / ITE / NEMA

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			5.10.2.1	rsuWsaIndex	
			5.10.2.2	rsuWsaPsid	
			5.10.2.10	rsuWsaOptions	
3.5.1.3.3.2.6	Report WSA Version Number	G.1			
			5.10.4	rsuWsaVersion	
3.5.1.3.3.3	Configure IEEE 1609.4 Communications Requirements				
3.5.1.3.3.3.1	Store the IEEE 1609.4 Configuration for a Radio	4.2.3			
			5.2.2	rsuRadioTable	
			5.2.2.1	rsuRadioIndex	
			5.2.2.2	rsuRadioDesc	
			5.2.2.8	rsuRadioCh1	
			5.2.2.9	rsuRadioCh2	
			5.2.2.10	rsuRadioTxPower1	
			5.2.2.11	rsuRadioTxPower2	
3.5.1.3.3.3.2	Store Radio Channel Access Mode	4.2.3			
			5.2.2	rsuRadioTable	
			5.2.2.1	rsuRadioIndex	
			5.2.2.7	rsuRadioChanMode	
3.5.1.3.4	Configure V2X Radio Transmitter Requirements				
3.5.1.3.4.1	Store Default Transmit Power	4.2.3			
			5.2.2	rsuRadioTable	
			5.2.2.1	rsuRadioIndex	
			5.2.2.10	rsuRadioTxPower1	
			5.2.2.11	rsuRadioTxPower2	
3.5.1.3.4.2	Report Maximum Number of V2X Antennas Supported	G.1			

© 2020 AASHTO / ITE / NEMA Copy per RTM Distribution Permission

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			5.16.1	maxRsuAntennas	
3.5.1.3.4.3	Store Antenna Gain and Cable Losses	4.2.3			
			5.16.2	rsuAntennaTable	
			5.16.2.1	rsuAntennaIndex	
			5.16.2.5	rsuAntGain	
3.5.1.3.4.4	Store Antenna Type	4.2.3			
			5.16.2	rsuAntennaTable	
			5.16.2.1	rsuAntennaIndex	
			5.16.2.6	rsuAntDirection	
3.5.1.4	Manage RSU Applications Requirements				
3.5.1.4.1	Manage RSU Application Requirements				
3.5.1.4.1.1	Install an RSU Application	4.2.6			
			5.14.9	rsuInstallUpdate	
			5.14.10	rsuInstallFile	
			5.14.11	rsuInstallPath	
			5.14.12	rsuInstallStatus	
			5.14.2	rsuFirmwareVersion	
			5.15.16	rsuSysDir	
			1201v03 - 2.2.3	globalModuleTable	
3.5.1.4.1.2	Report Software Update Status	G.1			
			5.14.12	rsuInstallStatus	
			5.14.13	rsuInstallTime	
			5.14.14	rsuInstallStatusMessage	
			5.14.15	rsuScheduledInstallTime	
3.5.1.4.2	Manage RSU Application Configuration Requirements				
3.5.1.4.2.1	Install a Configuration File	G.3			
			5.14.9	rsuInstallUpdate	
			5.14.10	rsuInstallFile	

Copy per RTM Distribution Permission
© 2020 AASHTO / ITE / NEMA

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			5.14.11	rsuInstallPath	
			5.14.12	rsuInstallStatus	
			5.14.2	rsuFirmwareVersion	
			5.15.16	rsuSysDir	
			1201v03 - 2.2.3	globalModuleTable	
3.5.1.4.2.2	Report Configuration File Update Status	G.1			
			5.14.12	rsuInstallStatus	
			5.14.13	rsuInstallTime	
			5.14.14	rsuInstallStatusMessage	
3.5.1.5	Manage Location Corrections Requirements				
3.5.1.5.1	Forward Location Corrections Data	4.2.3			
			5.5.2	rsuIFMStatusTable	
			5.5.2.1	rsuIFMIndex	
			5.5.2.2	rsuIFMPsid	
			5.5.2.3	rsuIFMTxChannel	
			5.5.2.4	rsuIFMEnable	
			5.5.2.5	rsuIFMStatus	
			5.5.2.8	rsuIFMPayload	
3.5.1.5.2	Use RTCM Corrections Data	4.2.3			
			5.5.2	rsuIFMStatusTable	
			5.5.2.1	rsuIFMIndex	
			5.5.2.2	rsuIFMPsid	
			5.5.2.3	rsuIFMTxChannel	
			5.5.2.4	rsuIFMEnable	
			5.5.2.5	rsuIFMStatus	
			5.5.2.8	rsuIFMPayload	
3.5.2	RSU Monitoring Requirements				
3.5.2.1	Determine RSU Operational Performance Status Requirements				

© 2020 AASHTO / ITE / NEMA Copy per RTM Distribution Permission

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
3.5.2.1.1	Report Time Elapsed Since RSU Power On	G.1			
			5.13.1	rsuTimeSincePowerOn	
3.5.2.1.2	Report Amount of Free Memory	G.1			
			UCD-SNMP 4.11.0	memTotalFree	
3.5.2.1.3	Report Instantaneous CPU Load	G.1			
			UCD-SNMP 11.9.0	ssCpuUser	
			UCD-SNMP 11.10.0	ssCpuSystem	
3.5.2.1.4	Report CPU Load Average - 15 Minutes	G.1			
			UCD-SNMP 10.1.3.3	laLoad	
3.5.2.1.5	Report CPU Load Average - 5 Minutes	G.1			
			UCD-SNMP 10.1.3.2	laLoad	
3.5.2.1.6	Report CPU Load Average - 1 Minute	G.1			
			UCD-SNMP 10.1.3.1	laLoad	
3.5.2.1.7	Report Storage Space Available	G.1			
			UCD-SNMP 9.1.7.1	dskAvail	
3.5.2.1.8	Report Number of Messages Exchanged	4.2.1			
			5.12.1	maxRsuMessageCountsByPsid	
			5.12.2	rsuMessageCountsByPsidTable	
			5.12.2.1	rsuMessageCountsByPsidIndex	
			5.12.2.2	rsuMessageCountsByPsidId	

Copy per RTM Distribution Permission
© 2020 AASHTO / ITE / NEMA

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			5.12.2.3	rsuMessageCountsByChannel	
			5.12.2.4	rsuMessageCountsDirection	
			5.12.2.5	rsuMessageCountsByPsidTime	
			5.12.2.6	rsuMessageCountsByPsidCounts	
			5.12.2.7	rsuMessageCountsByPsidRowStatus	
3.5.2.2	Report Mode of Operations	G.1			
			5.17.3	rsuModeStatus	
3.5.2.3	Determine RSU Clock Status Requirements				
3.5.2.3.1	Report RSU Clock Source	G.1			
			5.17.5	rsuClockSource	
3.5.2.3.2	Report RSU Clock Status	G.1			
			5.17.6	rsuClockSourceStatus	
3.5.2.3.3	Store Allowable RSU Clock Source Timeout	G.3			
			5.17.7	rsuClockSourceTimeout	
3.5.2.3.4	Store Allowable RSU Clock Source Queries	G.3			
			5.17.8	rsuClockSourceFailedQuery	
3.5.2.3.5	Store Allowable Time Deviation	G.3			
			5.17.9	rsuClockDeviationTolerance	
3.5.2.4	Determine RSU Location Requirements				
3.5.2.4.1	Report RSU Location	G.1			
			5.7.6	rsuGnssLat	
			5.7.7	rsuGnssLon	
			5.7.8	rsuGnssElv	
3.5.2.4.2	Report Positioning Status	G.1			
			5.3.1	rsuGnssStatus	

© 2020 AASHTO / ITE / NEMA Copy per RTM Distribution Permission

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
3.5.2.4.3	Store Allowable RSU Location Tolerance	G.3			
			5.7.9	rsuGnssMaxDeviation	
3.5.2.4.4	Report RSU Location Deviation	G.1			
			5.7.10	rsuLocationDeviation	
3.5.2.4.5	Report RSU Estimated Location Error	G.1			
			5.7.11	rsuGnssPositionError	
3.5.2.5	Monitor Network Interface Requirements				
3.5.2.5.1	Monitor Data Link Errors - Ethernet	G.1			
			RFC 3635	dot3StatsTable	
3.5.2.6	Report Number of Messages Exchanged by V2X Radio and PSID	4.2.1			
			5.12.2	rsuMessageCountsByPsidTable	
			5.12.2.1	rsuMessageCountsByPsidIndex	
			5.12.2.2	rsuMessageCountsByPsidId	
			5.12.2.3	rsuMessageCountsByChannel	
			5.12.2.4	rsuMessageCountsDirection	
			5.12.2.5	rsuMessageCountsByPsidTime	
			5.12.2.6	rsuMessageCountsByPsidCounts	
3.5.2.7	Determine Number of Active Radios	4.2.1			
			5.2.2	rsuRadioTable	
			5.2.2.1	rsuRadioIndex	
			5.2.2.3	rsuRadioEnable	
3.5.2.8	Determine RF Communications Range Requirements				

Copy per RTM Distribution Permission © 2020 AASHTO / ITE / NEMA

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
3.5.2.8.1	Determine Maximum Number of Communications Range Entries	G.1			
			5.13.5	maxRsuCommRange	
3.5.2.8.2	Report the RF Communications Distance - 1 Minute	4.2.4			
			5.13.6	rsuCommRangeTable	
			5.13.6.1	rsuCommRangeIndex	
			5.13.6.2	rsuCommRangeSector	
			5.13.6.3	rsuCommRangeMsgId	
			5.13.6.4	rsuCommRangeFilterType	
			5.13.6.5	rsuCommRangeFilterValue	
			5.13.6.6	rsuCommRange1Min	
			5.13.6.12	rsuCommRangeStatus	
3.5.2.8.3	Report the RF Communications Distance - 5 Minutes	4.2.4			
			5.13.6	rsuCommRangeTable	
			5.13.6.1	rsuCommRangeIndex	
			5.13.6.2	rsuCommRangeSector	
			5.13.6.3	rsuCommRangeMsgId	
			5.13.6.4	rsuCommRangeFilterType	
			5.13.6.5	rsuCommRangeFilterValue	
			5.13.6.7	rsuCommRange5Min	
3.5.2.8.4	Report the RF Communications Distance - 15 Minutes	4.2.4			
			5.13.6	rsuCommRangeTable	
			5.13.6.1	rsuCommRangeIndex	
			5.13.6.2	rsuCommRangeSector	
			5.13.6.3	rsuCommRangeMsgId	
			5.13.6.4	rsuCommRangeFilterType	

© 2020 AASHTO / ITE / NEMA Copy per RTM Distribution Permission

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			5.13.6.5	rsuCommRangeFilterValue	
			5.13.6.8	rsuCommRange15Min	
3.5.2.8.5	Report the Average RF Communications Distance - 1 Minute	4.2.4			
			5.13.6	rsuCommRangeTable	
			5.13.6.1	rsuCommRangeIndex	
			5.13.6.2	rsuCommRangeSector	
			5.13.6.3	rsuCommRangeMsgId	
			5.13.6.4	rsuCommRangeFilterType	
			5.13.6.5	rsuCommRangeFilterValue	
			5.13.6.9	rsuCommRangeAvg1Min	
3.5.2.8.6	Report the Average RF Communications Distance - 5 Minutes	4.2.4			
			5.13.6	rsuCommRangeTable	
			5.13.6.1	rsuCommRangeIndex	
			5.13.6.2	rsuCommRangeSector	
			5.13.6.3	rsuCommRangeMsgId	
			5.13.6.4	rsuCommRangeFilterType	
			5.13.6.5	rsuCommRangeFilterValue	
			5.13.6.10	rsuCommRangeAvg5Min	
3.5.2.8.7	Report the Average RF Communications Distance - 15 Minutes	4.2.4			
			5.13.6	rsuCommRangeTable	
			5.13.6.1	rsuCommRangeIndex	
			5.13.6.2	rsuCommRangeSector	
			5.13.6.3	rsuCommRangeMsgId	
			5.13.6.4	rsuCommRangeFilterType	
			5.13.6.5	rsuCommRangeFilterValue	
			5.13.6.11	rsuCommRangeAvg15Min	

Copy per RTM Distribution Permission
© 2020 AASHTO / ITE / NEMA

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
3.5.2.9	Determine Application Status	4.2.3			
			5.19.2	rsuAppConfigTable	
			5.19.2.1	rsuAppConfigID	
			5.19.2.4	rsuAppConfigState	
3.5.2.10	Retrieve Configuration Parameters Requirements				
3.5.2.10.1	Report the Internal Operating Temperature	G.1			
			5.13.2	rsuIntTemp	
3.5.2.10.2	Determine the Internal Operating Temperature Thresholds	G.1			
			5.13.3	rsuIntTempLowThreshold	
			5.13.4	rsuIntTempHighThreshold	
3.5.2.11	Report RSU Current Status Requirements				
3.5.2.11.1	Report RSU Current Overall Status	G.1			
			5.17.10	rsuStatus	
3.5.2.11.2	Report RSU Services Status Requirements				
3.5.2.11.2.1	Report RSU System Services Status	4.2.1			
			5.20.1	maxRsuServices	
			5.20.2	rsuServiceTable	
			5.20.2.1	rsuServiceID	rsuServiceID = 1
			5.20.2.2	rsuServiceName	
			5.20.2.3	rsuServiceStatus	
3.5.2.11.2.2	Report GNSS Service Status	4.2.1			
			5.20.1	maxRsuServices	
			5.20.2	rsuServiceTable	
			5.20.2.1	rsuServiceID	rsuServiceID = 2
			5.20.2.2	rsuServiceName	
			5.20.2.3	rsuServiceStatus	
3.5.2.11.2.3	Report Time Service Status	4.2.1			

© 2020 AASHTO / ITE / NEMA Copy per RTM Distribution Permission

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			5.20.1	maxRsuServices	
			5.20.2	rsuServiceTable	
			5.20.2.1	rsuServiceID	rsuServiceID = 3
			5.20.2.2	rsuServiceName	
			5.20.2.3	rsuServiceStatus	
3.5.2.11.2.4	Report Storage Service Status	4.2.1			
			5.20.1	maxRsuServices	
			5.20.2	rsuServiceTable	
			5.20.2.1	rsuServiceID	rsuServiceID = 4
			5.20.2.2	rsuServiceName	
			5.20.2.3	rsuServiceStatus	
3.5.2.11.2.5	Report Access Control Service Status	4.2.1			
			5.20.1	maxRsuServices	
			5.20.2	rsuServiceTable	
			5.20.2.1	rsuServiceID	rsuServiceID = 5
			5.20.2.2	rsuServiceName	
			5.20.2.3	rsuServiceStatus	
3.5.2.11.2.6	Report Network Service Status	4.2.1			
			5.20.1	maxRsuServices	
			5.20.2	rsuServiceTable	
			5.20.2.1	rsuServiceID	rsuServiceID = 6
			5.20.2.2	rsuServiceName	
			5.20.2.3	rsuServiceStatus	
3.5.2.11.2.7	Report Radio Access Service Status	4.2.1			
			5.20.1	maxRsuServices	
			5.20.2	rsuServiceTable	
			5.20.2.1	rsuServiceID	rsuServiceID = 7
			5.20.2.2	rsuServiceName	

Copy per RTM Distribution Permission
© 2020 AASHTO / ITE / NEMA

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			5.20.2.3	rsuServiceStatus	
3.5.2.11.2.8	Report V2X Radio Networking Services Status	4.2.1			
			5.20.1	maxRsuServices	
			5.20.2	rsuServiceTable	
			5.20.2.1	rsuServiceID	rsuServiceID = 8
			5.20.2.2	rsuServiceName	
			5.20.2.3	rsuServiceStatus	
3.5.2.11.2.9	Report IEEE 1609.2 Status	4.2.1			
			5.20.1	maxRsuServices	
			5.20.2	rsuServiceTable	
			5.20.2.1	rsuServiceID	rsuServiceID = 9
			5.20.2.2	rsuServiceName	
			5.20.2.3	rsuServiceStatus	
3.5.2.11.2.10	Report SCMS Service Status	4.2.1			
			5.20.1	maxRsuServices	
			5.20.2	rsuServiceTable	
			5.20.2.1	rsuServiceID	rsuServiceID = 10
			5.20.2.2	rsuServiceName	
			5.20.2.3	rsuServiceStatus	
3.5.2.11.2.11	Report Vendor Specific Services Status	4.2.1			
			5.20.1	maxRsuServices	
			5.20.2	rsuServiceTable	
			5.20.2.1	rsuServiceID	
			5.20.2.2	rsuServiceName	
			5.20.2.3	rsuServiceStatus	
3.5.2.11.2.12	Report RSU Services Description	4.2.1			
			5.20.1	maxRsuServices	
			5.20.2	rsuServiceTable	

© 2020 AASHTO / ITE / NEMA Copy per RTM Distribution Permission

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			5.20.2.1	rsuServiceID	
			5.20.2.4	rsuServiceStatusDesc	
3.5.2.11.2.13	Report RSU Services Status Update Time	4.2.1			
			5.20.1	maxRsuServices	
			5.20.2	rsuServiceTable	
			5.20.2.1	rsuServiceID	
			5.20.2.5	rsuServiceStatusTime	
3.5.3	RSU Control Requirements				
3.5.3.1	Control Mode of Operation	G.3			
			5.17.2	rsuMode	
3.5.3.2	Control RF Antenna Output	4.2.3			
			5.16.2	rsuAntennaTable	
			5.16.2.1	rsuAntennaIndex	
			5.16.2.5	rsuAntGain	
3.5.3.3	Reboot RSU	G.3			
			5.17.4	rsuReboot	
3.5.3.4	Control Application	4.2.3			
			5.19.2	rsuAppConfigTable	
			5.19.2.1	rsuAppConfigID	
			5.19.2.5	rsuAppConfigStart	
			5.19.2.6	rsuAppConfigStop	
3.5.4	Security Requirements				
3.5.4.1	Configure Security Requirements				
3.5.4.1.1	Configure Authentication Requirements				
3.5.4.1.1.1	Report Valid Geographic Region - Enrollment Certificates	G.1			
			5.9.3	rsuSecEnrollCertValidRegion	
3.5.4.2	Monitor Availability Requirements				

Copy per RTM Distribution Permission
© 2020 AASHTO / ITE / NEMA

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
3.5.4.2.1	Report Expiration Date - Enrollment Certificates	G.1			
			5.9.6	rsuSecEnrollCertExpiration	
3.5.4.2.2	Report Expiration Date - Application Certificates	4.2.1			
			5.9.9	maxRsuSecAppCerts	
			5.9.10	rsuSecAppCertTable	
			5.9.10.1	rsuSecAppCertIndex	
			5.9.10.2	rsuSecAppCertPsid	
			5.9.10.4	rsuSecAppCertExpiration	
3.6	Supplemental Non-communications Requirements				
3.6.1	Security Requirements				
3.6.1.1	Authenticate Authorized Messages Requirements				
3.6.1.1.1	Support SHA-1		NIST FIPS PUB 180-4		No Individual Object
3.6.1.1.2	Support SHA-2		RFC 7860		No Individual Object
3.6.1.2	Confidentiality Requirements				
3.6.1.2.1	Access RSU - USM		RFC 3414		No Individual Object
			RFC 5590		No Individual Object
3.6.1.2.2	Access RSU - TSM		RFC 5591		No Individual Object Note: When accessing the RSU with SNMPv3, TSM is to be used first, with USM as a fallback if one of the TSM services fail.
3.6.1.2.3	Support AES-256 Encryption		NIST FIPS PUB 197		No Individual Object
3.6.1.2.4	Support DTLS		RFC 6347		No Individual Object
			RFC 6353		No Individual Object

© 2020 AASHTO / ITE / NEMA Copy per RTM Distribution Permission

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
3.6.2	Response Time for Requests				See Requirement 3.6.3 in the PRL.
3.6.3	Event Log Data Requirements				
3.6.3.1	Event Log - System Events				The event log is required to contain the following fields. The event log may be compressed using a non-proprietary application (e.g., gzip).
			RFC 5424:6.2.1	PRI	
			RFC 5424:6.2.3	TIMESTAMP	In UTC and shall support TIME-SECFRAC with millisecond resolution
			RFC 5424:6.2.5	APP-NAME	Device or application
			RFC 5424:6.2.6	PROCID	e.g., Linux process ID.
			RFC 5424:6.4	MSG	Free-form message
3.6.3.2	Event Log - Application Events				The event log is required to contain the following fields. The event log may be compressed using a non-proprietary application (e.g., gzip).
			RFC 5424:6.2.1	PRI	
			RFC 5424:6.2.3	TIMESTAMP	In UTC and shall support TIME-SECFRAC with millisecond resolution
			RFC 5424:6.2.5	APP-NAME	Device or application
			RFC 5424:6.2.6	PROCID	e.g., Linux process ID.
			RFC 5424:6.4	MSG	Free-form message

Copy per RTM Distribution Permission
© 2020 AASHTO / ITE / NEMA

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
3.6.3.3	Event Log - RSU Configuration				The event log is required to contain the following fields. The event log may be compressed using a non-proprietary application (e.g., gzip).
			RFC 5424:6.2.1	PRI	
			RFC 5424:6.2.3	TIMESTAMP	In UTC and shall support TIME-SECFRAC with millisecond resolution
			RFC 5424:6.2.5	APP-NAME	Device or application
			RFC 5424:6.2.6	PROCID	e.g., Linux process ID.
			RFC 5424:6.4	MSG	Free-form message
3.6.3.4	Event Log - Notification				The event log is required to contain the following fields. The event log may be compressed using a non-proprietary application (e.g., gzip).
			RFC 5424:6.2.1	PRI	
			RFC 5424:6.2.3	TIMESTAMP	In UTC and shall support TIME-SECFRAC with millisecond resolution
			RFC 5424:6.2.5	APP-NAME	Device or application
			RFC 5424:6.2.6	PROCID	e.g., Linux process ID.
			RFC 5424:6.4	MSG	Free-form message
3.6.3.5	Event Log - Security				The event log is required to contain the following fields. The event log may be compressed using a non-proprietary application (e.g., gzip).
			RFC 5424:6.2.1	PRI	

© 2020 AASHTO / ITE / NEMA
Copy per RTM Distribution Permission

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
			RFC 5424:6.2.3	TIMESTAMP	In UTC and shall support TIME-SECFRAC with millisecond resolution
			RFC 5424:6.2.5	APP-NAME	Device or application
			RFC 5424:6.2.6	PROCID	e.g., Linux process ID.
			RFC 5424:6.4	MSG	Free-form message
3.6.3.6	Event Log - Stored Message				The event log is required to contain the following fields. The event log may be compressed using a non-proprietary application (e.g., gzip).
			RFC 5424:6.2.1	PRI	
			RFC 5424:6.2.3	TIMESTAMP	In UTC and shall support TIME-SECFRAC with millisecond resolution
			RFC 5424:6.2.5	APP-NAME	Device or application
			RFC 5424:6.2.6	PROCID	e.g., Linux process ID.
			RFC 5424:6.4	MSG	Free-form message
3.6.3.7	Event Log - Immediate Forward Message				The event log is required to contain the following fields. The event log may be compressed using a non-proprietary application (e.g., gzip).
			RFC 5424:6.2.1	PRI	
			RFC 5424:6.2.3	TIMESTAMP	In UTC and shall support TIME-SECFRAC with millisecond resolution
			RFC 5424:6.2.5	APP-NAME	Device or application
			RFC 5424:6.2.6	PROCID	e.g., Linux process ID.
			RFC 5424:6.4	MSG	Free-form message

Copy per RTM Distribution Permission
© 2020 AASHTO / ITE / NEMA

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
3.6.4	Interface Data Log Data Requirements				
3.6.4.1	Interface Data Log Format		libpcap v1.1.1 or later		No Individual Object SRD-USDOTRSE-003-ReqCML016v001 Communications Message Log Format in RSU v3.0 Specification. All transmitted and received 802.11p frames shall be stored in pcap format file (using libpcap, v1.1.1 or later for Unix based systems; or WinPcap v4.1.2 or later for Microsoft Windows based systems, or equivalent for other operating systems).
3.6.4.2	Interface Data Log File Format		libpcap v1.1.1 or later	Timestamps	
3.6.4.3	Interface Data Log File Naming Convention Requirements				
3.6.4.3.1	Support RSU Identifier in the Interface Data Log Filename		5.8.2.8	rsuIfaceLogName	This shall be the <identifier> field
3.6.4.3.2	Support Interface Identifier in the Interface Data Log Filename		5.8.2.8	rsuIfaceLogName	This shall be the <interface> field
3.6.4.3.3	Support Direction in the Interface Data Log Filename		5.8.2.8	rsuIfaceLogName	This shall be the <direction> field
3.6.4.3.4	Support Date and Time in the Interface Data Log Filename		5.8.2.8	rsuIfaceLogName	This shall be the <time> field
3.6.4.4	Interface Data Logging - Operational State		5.17.3	rsuModeStatus	
3.6.4.5	Open a New Interface Data Log		5.8.2	rsuInterfaceLogTable	
			5.8.2.1	rsuIfaceLogIndex	
			5.8.2.3	rsuIfaceMaxFileSize	
			5.8.2.4	rsuIfaceMaxFileTime	

© 2020 AASHTO / ITE / NEMA Copy per RTM Distribution Permission

Requirements Traceability Matrix (RTM)					
FR ID	**Functional Requirement**	**Dialog ID**	**Object ID**	**Object Name**	**Additional Specifications**
3.6.5	Copy Files using SCP	4.2.5			Note: Check for the latest security patches for SCP.
3.6.6	User Accounts				See Requirement 3.6.6 in the PRL
3.6.7	Time Fix - Alternating Mode				See Requirement 3.6.7 in the PRL
3.6.8	Determine Maximum Number of Application Certificates Supported				See Requirement 3.6.8 in the PRL

Copy per RTM Distribution Permission
© 2020 AASHTO / ITE / NEMA

Annex B
Object Tree [Informative]

Figure 7 provides a pictorial representation of the Roadside Unit Object Tree Structure. The tree structure identifies how the object definitions are combined under specific nodes.

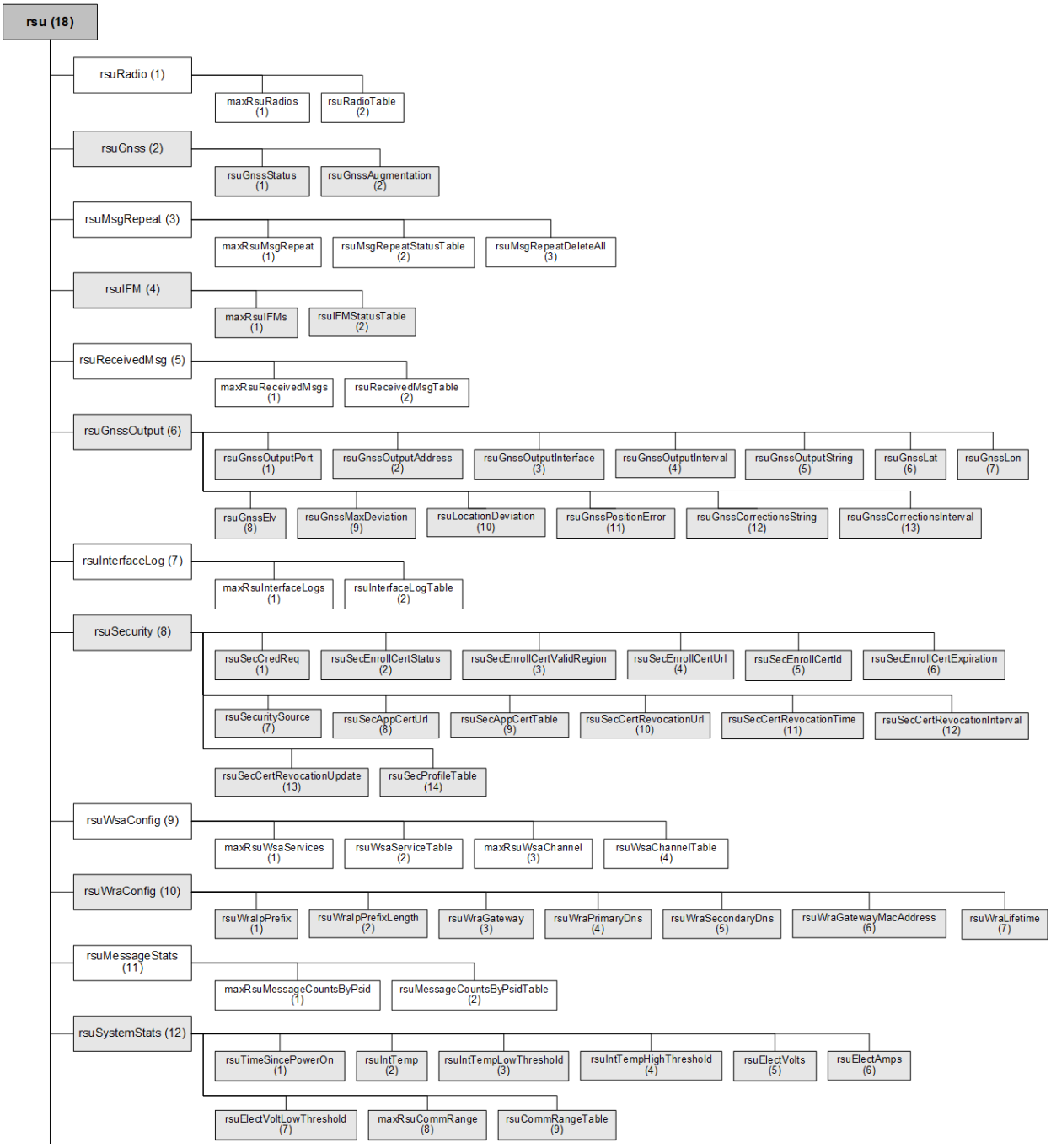

Figure 7 Object Tree for NTCIP 1218 v01

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

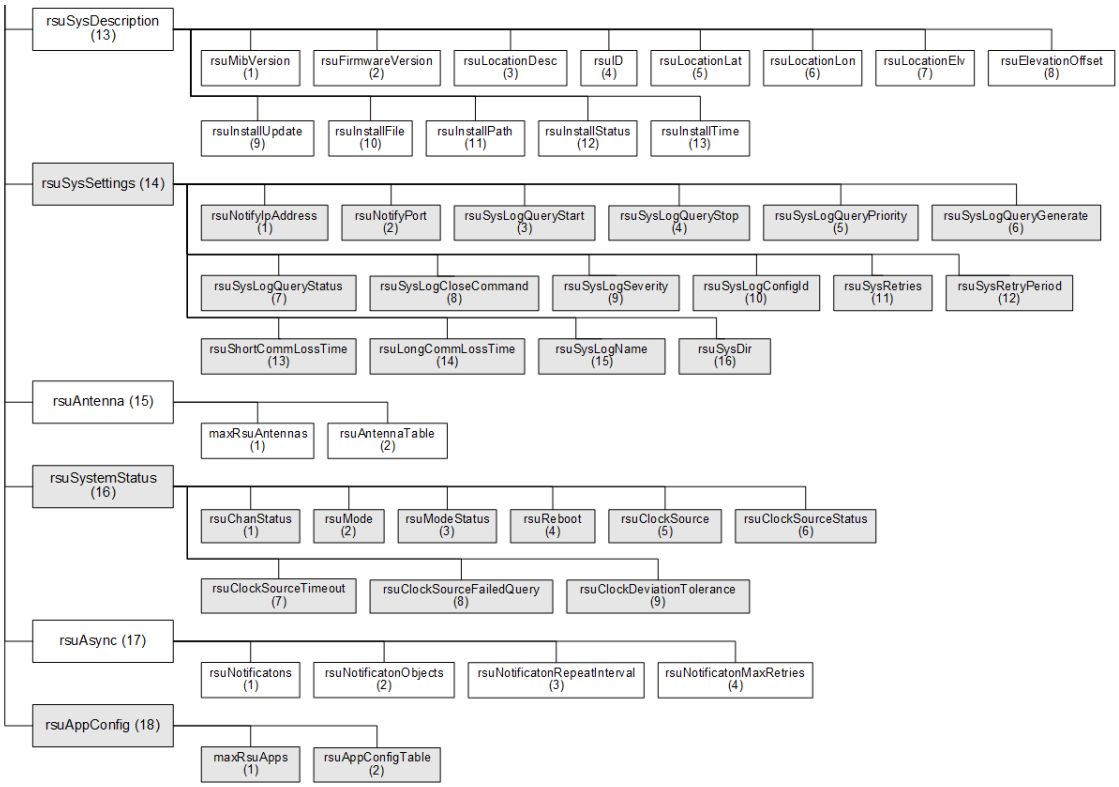

Figure 7 (Continued) Object Tree for NTCIP 1218 v01

© 2020 AASHTO / ITE / NEMA

Annex C
Test Procedures [Normative]

It is anticipated that Test Procedures may be developed as part of a future revision of NTCIP 1218 v01. Annex C is a placeholder, at present.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

Annex D
Documentation of Revisions [Informative]

Annex D is reserved for the documentation of revisions in future versions of NTCIP 1218 v01.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

Annex E
User Requests [Informative]

Annex E identifies features that were suggested for NTCIP 1218 v01, but are either supported by mechanisms that may not be readily obvious, or are not supported by NTCIP 1218 v01.

E.1 Approach

The Systems Engineering Management Plan for this project identifies the following objectives for NTCIP 1218 v01: For a management station to configure the RSU to:

a) Collect BSM related information
b) Receive data (e.g. SPaT/MAP) from a signal controller
c) Transmit (send) data to a signal controller
d) Transmit alerts and traveler information to vehicles
e) Transmit SPaT/MAP data to connected vehicles
f) Coordinate signal prioritization between connected vehicles and controllers
g) Collect traffic performance measure data
h) Monitor and log RSU operational data
i) Manage and operate the interface with the SCMS.

However, NTCIP 1218 v01 strives to be agnostic and several of the identified objectives are information specific (i.e., reference SAE J2735 messages) or implementation specific (e.g., SCMS, signal controllers). NTCIP 1218 v01 focuses on meeting these objectives without referencing a specific standard or implementation.

E.2 Perform Diagnostics

This was identified as a potential user need but the NTCIP RSU WG was unable to clearly articulate what type of diagnostics was needed.

E.3 Manage RSU Initialization Functions

The NTCIP RSU WG originally identified a user need to retrieve and configure the initialization functions for the RSU. The initialization functions are performed after an electrical power reboot and may be defined by a bootstrap. However, during the requirements definition phase, the NTCIP RSU WG determined that the requirements for this user need are better addressed in a future RSU specification (or standard) at this time. The user needs and requirements text follow.

E.3.1 User Need - Manage RSU Initialization Functions

The NTCIP RSU WG originally identified a user need to retrieve and configure the initialization functions for the RSU. The initialization functions are performed after an electrical power reboot and may be defined by a bootstrap. However, during the requirements definition phase, the NTCIP RSU WG determined that the requirements for this user need are better addressed in a future RSU specification (or standard) at this time.

E.3.2 Requirement - Mandatory Applications

Upon request from a management station, the RSU shall store what mandatory applications are part of the RSU's initialization functions.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

E.4 RSU Master - Slave

The NTCIP RSU WG originally identified a user need to configure an RSU to be part of a coordinated group of RSUs, based on the features identified in RSU 4.1 Spec. This user need allows a set of RSUs to exchange data as a single unit. Multiple RSUs may be needed to extend the wireless communications coverage at a location, such as a signalized intersection that covers a large geographic area or an area with line-of-sight problems (e.g., trees). This feature also allows the RSUs to manage the messages that may be received by the set of RSUs to act as one unit so that a message is sent only once to a network destination (by a designated unit) to conserve bandwidth. In this scenario, the designated RSU becomes the basis for the configuration for the RSUs that together operates as a single unit. However, during the requirements definition phase, the NTCIP RSU WG determined that a TMC can better manage and operate the RSU master/client relationship and synchronization than trying to configure and manage synchronization among the RSUs. Four requirements were derived from this user need. The requirements text follows.

E.4.1 Requirement - Store RSU Master - Slave Assignment

Upon request by a management station, the RSU shall store if it is part of a set of RSUs. A set of RSUs are multiple RSUs that act as a single unit for purposes of exchanging data with a management station and other external devices.

E.4.2 Requirement - Store RSU Master - Slave Role

If an RSU is part of a set of RSUs deployed as a single unit, upon request by a management station, the RSU shall store if it is the master unit or slave unit. For a set of RSUs, the master unit acts as the single point of contact with the management station and other external devices. Slave units for a set of RSUs are configured based on the configuration of the master unit. The messages to be stored and forwarded to the wireless interface; and messages received from the wireless interface. The operating channels for radios operating on alternating mode.

E.4.3 Requirement - Store RSU Slave Address

Upon request by a management station, an RSU that is a master unit for a set of RSUs shall store the network addresses of the slave units. Slave units in a set of RSUs are expected to receive messages for forwarding to the wireless interface from the master unit and to forward messages received from the wireless interface to the master unit. Where necessary, specify IPv6 network address.

E.4.4 Requirement - Store RSU Master Address

Upon request by a management station, an RSU that is a slave unit for a set of RSUs shall store the network address of the master unit.

E.5 Report Firmware Update Status Options

For requirement 3.5.1.1.5.3, Report Firmware Update Status, the NTCIP RSU WG considered allowing an implementation to define other options than to roll-back the RSU firmware to the pre-update version, but the options could not be clearly defined at the time, so the requirement was removed.

E.6 Encrypting Messages Transmitted Over the V2X Interface

The NTCIP RSU WG considered support to encrypt messages transmitted over the V2X Interface. A requirement is included in NTCIP 1218 v01 to support if a message to be transmitted over the V2X interface is to be encrypted, but NTCIP 1218 v01 does not define HOW the payload of a message is to be encrypted (i.e., what encryption algorithm to use). Based on the encryption algorithm to be used,

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

additional parameters may need to be defined, such as management of encryption keys. This may be a function of the application.

E.7 Signing Messages Transmitted Over the V2X Interface

The NTCIP RSU WG considered support to sign messages transmitted over the V2X Interface. A requirement is included in NTCIP 1218 v01 to support if a message to be transmitted over the V2X interface is to be signed, but NTCIP 1218 v01 does not define HOW the payload of a message is to be signed (i.e., what signing mechanism is to be used, what SSPs are to be assigned). This may be a function of the application.

E.8 Encoding Messages Transmitted Over the V2X Interface

The NTCIP RSU WG considered support to encode messages transmitted over the V2X Interface. A requirement is included in NTCIP 1218 v01 to support if a message to be transmitted over the V2X interface is to be encoded, but NTCIP 1218 v01 does not define HOW the payload of a message is to be encoded (i.e., how is the message is to be encoded). For example, there are different levels of encoding - IEEE 1609.2 encoding, or UPER encoding. This may be a function of the RSU application to determine the encoding for the message.

E.9 Manage Scheduler

The NTCIP RSU WG originally identified a user need to retrieve and configure a scheduler in the RSU to implement features available to the manager based on time. However, during the requirements phase, the NTCIP RSU WG determined that requirements already existed in NTCIP 1218 v01 for specific scheduling needs (such as transmitting a stored message) or can be addressed by a generic scheduler by the RSU's operating system.

Note: need to schedule interface log data

E.10 Security

NTCIP 1218 v01 addresses only those security requirements that address the machine-to-machine interface between the management station and the RSU; and can be managed via a MIB. The NTCIP RSU WG originally considered other additional requirements, as described by numerous cybersecurity documents, such as:

a) Draft NIST Special Publication (SP) 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations
b) ISO/TS 21177:2019, Intelligent transport systems - ITS-station security services for secure session establishment and authentication between trusted devices.

However, the NTCIP RSU WG agreed that requirements that do not meet the described criteria belong in a specification and not in NTCIP 1218 v01. For example, RFC 6347 TLS version 1.2 can satisfy many of the requirements, and can be configured, but needs to be managed by a mechanism outside a MIB. In addition, for example, NCCIC Alert TA17-156A provides information about reducing the risk of SNMP abuse.

E.11 RSU Component Information

The NTCIP RSU WG identified a requirement to determine if a RSU component is trusted or certified, but the mechanism on how to identify trust or certification is ambiguous at the time. Thus the RSU WG decided not to include the requirement at this time. The requirement text follows.

Requirement - RSU Component Information Certification

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

> Upon request from a management station, the RSU shall indicate if the component (e.g., hardware model, software version) is trusted or certified (e.g., by a testing laboratory). If the component is trusted or certified, the management station should return an identifier of the certification (e.g., certificate number).

E.12 RSU Edge Computing

The NTCIP RSU WG considered user needs to process data received by the RSU via the V2X interface, such as the data in Basic Safety Messages received by the RSU. Such edge computing may pre-process the data, then transmit the processed data to a management station. The purpose of the edge computing is to reduce the amount of data to be forwarded to a management station. The NTCIP RSU WG considered such processing as an application, and so is outside the scope of NTCIP 1218 v01.

E.13 RSU Firmware Update of Mobile Devices

The NTCIP RSU WG considered a user need to manage updating the firmware of mobile devices, such as OBUs. However, the NTCIP RSU WG considered such a process to be an application, and thus outside the scope of NTCIP 1218 v01.

E.14 Valid Geographic Region for Application Certificates

The NTCIP RSU WG considered a requirement regarding the validity of application certificates based on the geographic location of the RSU. However, how the geographic location can be defined in a standardized format is still ambiguous. Thus, the requirement that the NTCIP RSU WG agreed to defer follows:

> Upon request from a management station, the RSU shall store the valid geographic region for application certificates. Application certificates may define a geographic region within which the certificate is valid. This requirement allows the RSU to define a valid geographic region, which is within the radius of the RSU's location in meters, so the RSU requests, receives and stores application certificates with the appropriate geographic region.

E.15 Event Log - User-Defined Events

The NTCIP RSU WG considered requirements to allow a transportation manager to define user-defined events to be logged in the RSU's system log (syslog). Upon further discussion, the NTCIP RSU WG determined that at the current time, these user-defined events should be defined by the specific applications on the RSU. However, as additional experience with RSUs is gained, the NTCIP RSU WG may wish to revisit these requirements.

E.15.1 Requirement - Event Log - Configure User-Defined Events

Upon request from a management station, the RSU shall store a user-defined event that results in an entry in the RSU's event log. The user-defined event is defined by a specific change to the value of a data object defined by NTCIP 1218 v01. The allowable specified changes, if supported by the RSU, are:

a) On-change Event - monitor the data element for changes in value
b) Greater Than Event - monitor the data element for values exceeding a defined threshold
c) Less Than Event - monitor the data element for values falling below a defined threshold
d) Hysteresis Event - monitor the data element for values exceeding an upper limit or dropping below a lower limit
e) Periodic Event - monitor the data element and transmit a notification at user-defined intervals
f) Bit Flag Event - monitor the data element for one or more bits of a value becoming true (i.e., obtaining a value of one)

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

E.15.2 Requirement - Event Log - User-Defined Events

When a user-defined event defined by a specific change to the value of a data object defined by NTCIP 1218 v01 occurs, the RSU shall write an entry in its event log.

E.15.3 Requirement - Event Log - Configure User-Defined Conditions - Received Message on the V2X Interface

Upon request from a management station, the RSU shall store the user-defined conditions for a message received on the V2X interface that result in an entry in the RSU's event log. The user-defined conditions are defined by specific values of the contents of a message received by the RSU via the V2X interface.

E.15.4 Requirement - Event Log - User-Defined Conditions - Received Messages on the V2X Interface

When the user-defined conditions for a message received on the V2X interface are satisfied, the RSU shall write an entry in its event log. The user-defined conditions are defined by specific values of the contents of a message received by the RSU via the V2X interface.

E.15.5 Requirement - Event Log Priority Levels

All event log entries in the RSU's event log shall contain a logging priority level, as defined in RFC 3164.

E.15.6 Supplemental Requirement - Record and Timestamp Events

The RSU shall support the capability to record configured user-defined event types with timestamps in the event log.

E.15.7 Supplemental Requirement - Support On-Change Events

Upon request from a management station, the RSU shall allow any event type configuration to monitor data for changes in values.

E.15.8 Supplemental Requirement - Support Greater Than Events

Upon request from a management station, the RSU shall allow any event type configuration to monitor data for values exceeding a defined threshold for a period of time.

E.15.9 Supplemental Requirement - Support Less Than Events

Upon request from a management station, the RSU shall allow any event type configuration to monitor data for values falling below a defined threshold for a period of time.

E.15.10 Supplemental Requirement - Support Hysteresis Events

Upon request from a management station, the RSU shall allow any event type configuration to monitor data for values exceeding an upper limit or dropping below a lower limit.

E.15.11 Supplemental Requirement - Support Periodic Events

Upon request from a management station, the RSU shall allow any event type configuration to monitor data on a periodic basis.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

E.15.12 Supplemental Requirement - Support Bit Flag Events

Upon request from a management station, the RSU shall allow any event type configuration to monitor one or more bits of a value becoming true (e.g., obtaining a value of one).

E.15.13 Supplemental Requirement - Support Event Monitoring on Any Data

Upon request from a management station, the RSU shall allow a management station to configure any event type to monitor any piece of data supported by the RSU within the logical rules of the type of event (e.g., ASCII strings should not be monitored with greater than or less than conditions).

Note: This allows a user to monitor an event based on the value of any data.

E.16 Requirement - Device Installation Date

The NTCIP RSU WG considered a requirement to determine the installation date of the RSU device, however agreed to reconsider this requirement in the future. This requirement may be more appropriate in NTCIP 1201, Global Object Definitions, or in a future RSU specification (or standard).

E.17 Requirement - Encoding Formats

The NTCIP RSU WG considered a requirement to support different formats and encoding schemes for (Store and Repeat, Immediate Forward) message payloads for transmission through the V2X Interface. Formats considered were ASN.1, XML Encoding Rules (XER) and JSON Encoding Rules (JER). The default format is the format defined in USDOT's RSU 4.1 Spec Appendix C (UPER encoded + additional fields). However, the NTCIP RSU WG agreed to table this requirement for future consideration.

E.18 UDP Port for Immediate Forwarding

USDOT's RSU 4.1 Spec requirement 544-v01 requires that the RSU listen to UDP port 1516. However, this requirement enables a security hole in the RSU in that the RSU is required to listen to all messages sent to that port and allows the RSU to transmit malicious content. The NTCIP RSU WG recommends that this requirement be removed from a future version of USDOT RSU 4.1 Spec.

E.19 Clock Skew Rate

USDOT's RSU 4.1 Spec requirement 618-v002 requires that the RSU notify a remote host if the value of the internal clock drift (skew) rate has exceeded a configurable tolerance. The NTCIP RSU WG considered 2 similar requirements for a clock skew rate in NTCIP 1218 v01. These requirements were:

a) Upon request from a management station, the RSU shall store the allowable clock drift (skew rate), in milliseconds over a user-defined time period, on the RSU. The clock drift is the difference between the RSU's system clock and the current clock source the last time the system clock was synchronized with the time source. If the clock drift exceeds the allowable value over that user-defined time period, then the RSU clock status is to indicate a clock drift error.
b) The RSU shall transmit a notification to the destination network address and port number upon detection of a clock skew rate greater than a defined threshold.

However, the NTCIP RSU WG did not agree on what that user-defined time period should be. An RSU is expected to update its system clock at regular intervals based on how often it receives a GNSS time source. While a transportation manager may wish to determine it a RSU's system clock has a high drift (skew rate), the RSU continuously updates its system clock based on GNSS time, and NTCIP 1218 v01 defines other requirements for other notifications if the GNSS time source is lost (see Section 3.5.1.1.7.3.6) or if the differences between two clock sources exceed a user-defined threshold (see Section 3.5.1.1.7.3.7).

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

E.20 Radios Broadcasting on the Same Channel

The NTCIP RSU WG considered a requirement to prevent more than one V2X radio from broadcasting on a communications channel. However, this requirement was determined to belong in a future RSU specification (or standard) and was not included in NTCIP 1218 v01.

E.21 Monitor Electrical Power

The NTCIP RSU WG considered a user need to monitor the electrical power to the RSU such as voltage. Requirements were developed including a design. However, this feature is not currently implemented on RSUs and is not currently part of any known agency specification so the NTCIP RSU WG agreed to table this user need for future consideration. The original user need was:

> A transportation operator needs to monitor the electrical power to the RSU such as voltage. This feature allows an operator to retrieve the history of any power interruptions and nominal operating voltage, if the RSU is equipped.

E.21.1 Requirement - Monitor Electrical Voltage

Upon request from a management station, the RSU shall report its nominal operating voltage, in volts, from 0 volts to 254 volts.

E.21.2 Requirement - Monitor Electrical Current

Upon request from a management station, the RSU shall report the amount of current the RSU is drawing, in milliampere (mA) units.

E.21.3 Requirement - Determine Electrical Voltage Threshold

Upon request from a management station, the RSU shall report the low electrical voltage threshold, in volts. The RSU is to transmit a notification if the operating voltage drops below this threshold.

E.21.4 Object Definition - RSU Electrical Voltage

```
rsuElectVolts OBJECT-TYPE
    SYNTAX       Integer32 (0..255)
    UNITS        "volt"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Contains the nominal operating voltage in
        volts, as measured by the RSU.
        <Valid Value Rule> Values 0 to 253 indicates valid values. Value 254
        indicates a voltage of 254 or greater. The value 255 indicates an
        error condition or missing value."
    DEFVAL       { 255 }
```

E.21.5 Object Definition - RSU Electrical Amperage

```
rsuElectAmps OBJECT-TYPE
    SYNTAX       Integer32 (0..2551)
    UNITS        "milliampere"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Contains the amount of current the RSU is
        drawing, in milliampere (mA) units.
```

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

```
        <Valid Value Rule> Values 0 to 2550 indicates valid values. Value
        2550 indicates a current of 2550 mA or greater. The value 2551
        indicates an error condition or missing value."
    DEFVAL       { 2551 }
```

E.21.6 Object Definition - RSU Electrical Voltage - Low Voltage Warning

```
rsuElectVoltLowThreshold OBJECT-TYPE
    SYNTAX       Integer32 (0..255)
    UNITS        "volt"
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> Indicates the low value of the operating
        voltage, in volts, associated with the internal voltage sensor below
        which would generate a notification. A value of 254 represents a
        voltage of 254 or higher. A value of 255 represents unknown."
    DEFVAL       { 255 }
```

E.22 Notification - Certificate Management Warnings

The NTCIP RSU WG considered a requirement for the RSU to transmit a notification a user-defined period prior to the expiration of current certificates or the RSU expects to be out of valid certificates. However, the appropriate functionality for this requirement is not defined at this time, so the NTCIP RSU WG agreed to table this requirement for future consideration. This functionality should be considered in a future RSU specification (or standard).

E.23 IEEE 802.1X

The NTCIP RSU WG considered an optional requirement to support IEEE 802.1X. This functionality would specify a common method and protocol to secure communications between authenticated devices. However, the NTCIP RSU WG agreed that IEEE 802.1X is not common for ITS field devices at this time, but merits further investigation and to table this requirement for future consideration. It was noted that several agencies currently do require IEEE 802.1X for its switches, but not necessarily for its ITS field devices at this time.

E.24 Factory Default

The NTCIP RSU WG considered an optional requirement to allow a management station to reset a RSU to its factory default. However, at the time of publication, efforts were started to develop a hardware standard for the RSU, and the NTCIP RSU WG was of the opinion that the proposed hardware standard should support the capability to reset the RSU to its hardware factory default.

E.25 Forwarding Messages Received from or Transmitted to the V2X Interface using TCP

The NTCIP RSU WG considered an option to support TCP as a transport protocol for forwarding messages received by or transmitted by the RSU over the V2X interface. However, at the time of publication, all implementations were using udp (and should be with a secured connection), and it was agreed that if tcp was used, the framing should be defined for interoperability purposes but there was insufficient data on how to frame it. Thus, the tcp option was deferred, and 5.6.2.5 rsuReceivedMsgProtocol and 5.21.2.5 rsuXmitMsgFwdingProtocol each have only two values at this time: other (1), and udp (2).

E.26 Standalone Mode

The NTCIP RSU WG considered an option to support standalone mode as a possible value for current mode of operation. In 'standalone' mode, the RSU's V2X radio and system logging is enabled, but periodic communications with a management station (e.g., an operations center) is not expected. In this

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

mode, the RSU operates with applicable functionality until the RSU's certificates expire. However, the NTCIP RSU WG was unable to define what functionality was available or unavailable during this mode. Also, functionality was added, in the form of short-term communications event and long-term communication event, that controls the behavior of the RSU if periodic communications with the management station is not expected.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

Annex F
Generic Concepts and Definitions

Annex F is a placeholder, at present.

Do Not Copy Without Written Permission © 2020 AASHTO / ITE / NEMA

Annex G
SNMP Interface [Normative]

Annexes G.1 through G.4 provide a description of the key services offered by SNMP assuming no errors.

Annex G.5 extends the requirements of NTCIP 1103 v03 by providing additional requirements that supplement, but do not replace any requirements of NTCIP 1103 v03.

G.1 Generic SNMP Get Interface

SNMP defines a generic process by which a management station can retrieve data from a device. This process consists of a Get request (GET) and a GetResponse as depicted in Figure 8. Both the Get request and the GetResponse messages contain a list of objects as defined by the varBindingList structure (see Annex G.4).

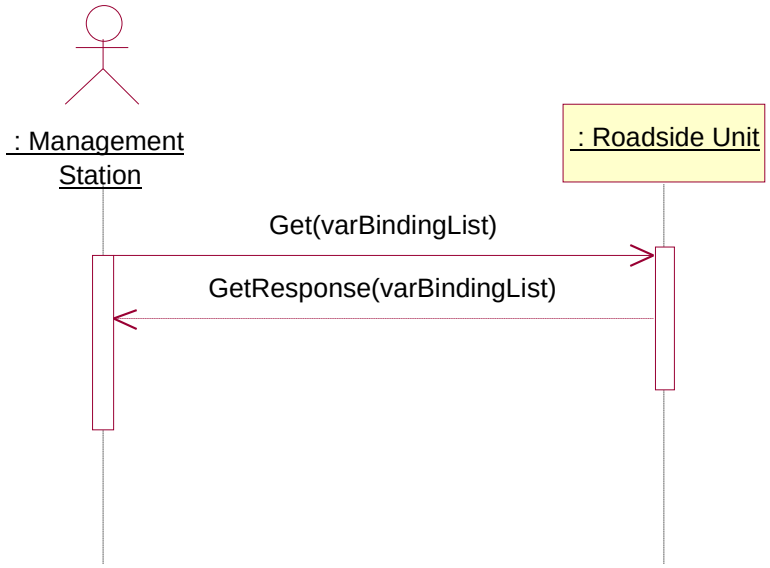

Figure 8 SNMP Get Interface

This generic process is customized by subsequent sections of NTCIP 1218 v01, by referencing the ‘GET’ operation, and directly by the RTM, by section number, to fulfill a wide range of the requirements defined in Section 3.

G.2 Generic SNMP Get-Next Interface

SNMP defines a process by which a management station can explore data within a device to fulfill the requirement as defined in Section 3. This process consists of a GetNext request and a GetResponse as depicted in Figure 9. Both the GetNext request and the GetResponse messages contain a list of objects as defined by the varBindingList structure (see Annex G.4).

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

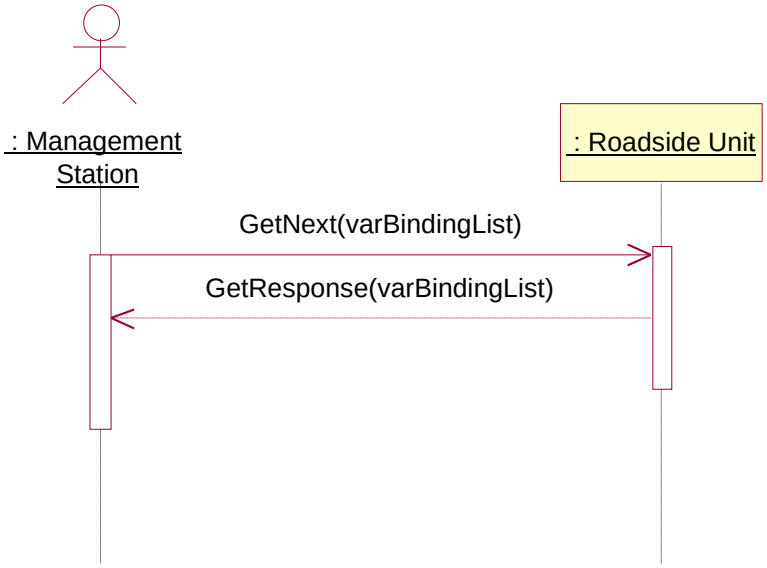

Figure 9 SNMP GetNext Interface

G.3 Generic SNMP Set Interface

SNMP defines a generic process by which a management station can transmit (send) data to a device. This process consists of a Set request and a GetResponse (sic) as depicted in Figure 10. Both the Set request and the GetResponse messages contain a list of objects as defined by the varBindingList structure (see Annex G.4).

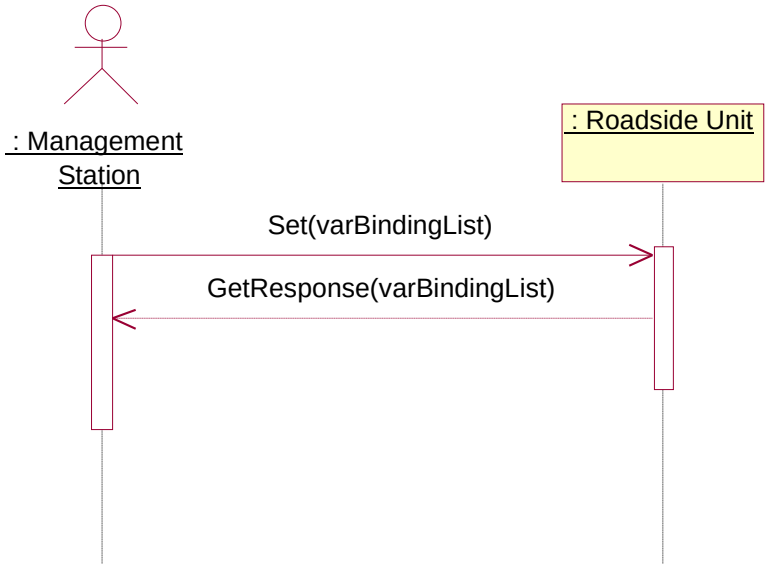

Figure 10 SNMP Set Interface

Note: The response message issued to an SNMP Set request is the same message structure as used to respond to an SNMP Get request. The SNMP standard calls this response message a GetResponse, but it is in fact a response to either a GET or a SET.

© 2020 AASHTO / ITE / NEMA

This generic process is customized by subsequent sections of NTCIP 1218 v01, by referencing the 'SET' operation, and directly by the RTM, by section number, to fulfill a wide range of the requirements defined in Section 3. Additional rules for SETs are defined by the Control Mode State Machine.

G.4 Variable Binding List Structure

The requests and responses for the Get, Get Next and Set operations, all use the varBindingList structure. RFC 3416 defines this structure as containing zero or more varBindings, where each varBinding is defined to consist of an object name (as indicated by an Object Identifier (OID)) and the associated object value. This relationship is depicted in Figure 11.

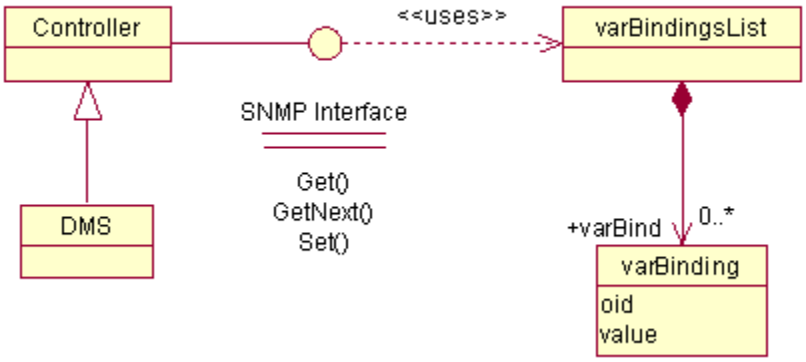

Figure 11 SNMP Interface - View of Participating Classes

G.5 Additional Requirements

G.5.1 Grouping of Objects in a Request

The RSU shall allow the management station to perform a single Get, GetNext, or Set operation on any combination of supported objects with the objects listed in any order within the message, unless otherwise restricted by NTCIP 1218 v01.

The RSU shall not associate any semantics to the ordering of objects within the varBindingsList. As required by RFC 3416 Section 4.2.5, each object shall be affected "as if simultaneously set with respect to all other assignments specified in the same message."

G.5.2 Support of Get

The RSU shall allow the management station to perform the Get operation on any supported object for which support for the Get Operation is indicated in Annex G.4.

G.5.3 Support of Get-Next

The RSU shall allow the management station to perform the GetNext operation on any OBJECT IDENTIFIER.

G.5.4 Support of Set

The RSU shall allow the management station to perform the Set operation on any supported object for which support for the Set Operation is indicated in Annex G.4.

© 2020 AASHTO / ITE / NEMA Do Not Copy Without Written Permission

G.5.5 Performance

The RSU shall process the Get, GetNext, or Set request in accordance with all of the rules of RFC 3416, including updating the value in the database and initiating transmission of the appropriate response (assuming that the RSU has permission to transmit) within 1 second of receiving the last byte of the request.

> Note: If a user desires a shorter response time, the user specifies this in the agency procurement specification.

G.5.6 Properly Defined Objects

Every supported object shall be defined in a manner that conforms to RFC 2578 and shall have a unique OBJECT IDENTIFIER properly registered under the ISO Naming Tree. If the definition of the supported object is controlled by parties within the ITS community, the object definition should also be consistent with NTCIP 8004 v02.

G.6 Generic SNMP Trap Interface

SNMP defines a generic process by which an agent, such as a roadside device, can generate and transmit information to a management station, based on the occurrence of specific events or conditions. This process consists of a Trap, as defined in Section 4.2.6 in RFC 3416 and depicted in Figure 12. The Trap message contains a list of objects as defined by the varBindingList structure (see Annex G.4).

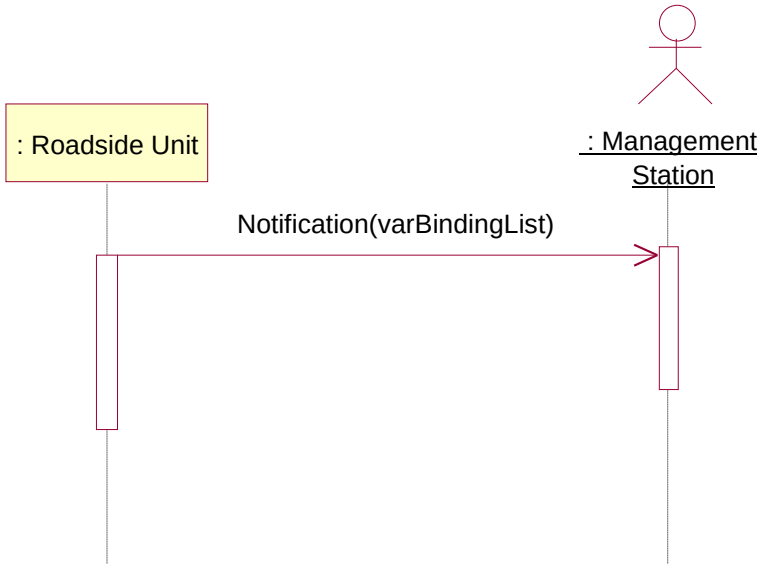

Figure 12 SNMP Trap Interface

This generic process is customized by sections of NTCIP 1218 v01, by referencing the ‘Notification’ operation, and directly by the RTM, by section number, to fulfill a wide range of the requirements defined in Section 3.

§

 © 2020 AASHTO / ITE / NEMA