Roadside Unit (RSU) Standard Draft

A connected intersection-ready Recommended Standard (RS) of AASHTO, ITE and NEMA

This is a draft document, produced by the RSU Standardization Working Group, which is distributed for review, vote/acceptance, and comment purposes only. You may reproduce and distribute this document within your organization but only for the purposes of and only to the extent necessary to facilitate review, vote/acceptance, and comment. Please ensure that all copies reproduced or distributed bear this notice.

This document contains preliminary information that is subject to change. When the standard is published, it will supersede the USDOT's DSRC Roadside Unit (RSU) Specifications Document v4.1.

Supported/Sponsored By: The United States Department of Transportation (USDOT)

Foreword

This Roadside Unit (RSU) Standard v01 supersedes USDOT's Dedicated Short-Range Communications Roadside Unit Specifications v4.1. This RSU Standard v01 was developed by engaging with stakeholders representing the industry at large including but not limited to infrastructure owner operators, automobile original equipment manufacturers, RSU manufacturers, and the end users of data and services. The work was supported by the United States Department of Transportation (USDOT) Intelligent Transportation Systems (ITS) Joint Program Office (JPO). Several associations such as the American Association of State Highway Transportation Officials (AASHTO), the Institute of Transportation Engineers (ITE), the National Electrical Manufacturers Associations (NEMA), and SAE International were involved in ensuring a balanced and effective stakeholder representation and adherence to standards development processes as Standards Development Organizations (SDOs).

This document establishes a non-proprietary, industry-based consensus Roadside Unit (RSU) Standard. An RSU is a transportation infrastructure communications device that is a part of a Cooperative Intelligent Transport Systems (C-ITS) transportation environment. The goal of such an environment is to reduce the number of fatalities and injuries on roadways, improve mobility and reduce environmental impacts. Commonly known as Connected Vehicles (CV) in the United States, terms such as Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) have been used to reflect the types of communications used. The vision for this technology has expanded to include all types of travelers including pedestrians, cyclists, and multimodal travelers and is referred to as Vehicle-to-Everything (V2X) technology and V2X communications.

More information on this standards effort can be found on the ITE Website.

The Standards Development Organizations (SDOs) supporting this standard include the following:

ITE

Siva Narla, snarla@ite.org
Tatiana Richey, trichey@ite.org
Nicola Tavares, standards@ite.org

AASHTO

Venkat Nallamothu
Strat Cavros, scavros@aashto.org

NEMA

Jean Johnson
Steve Griffith, steve.griffith@nema.org
Kezhen Shen, kezhen.shen@nema.org

SAE International

Keith Wilson, keith.wilson@sae.org

IEEE 1609 Working Group

Justin McNew, justinm@jmcrota.com
William Whyte, wwhyte@qti.qualcomm.com

RSU Standardization Working Group Co-chairs

Blaine Leonard, Utah Department of Transportation, AASHTO
Justin McNew, JMC Rota Inc., IEEE 1609/SAE

RSU Standardization Working Group (WG) Members

Alan Davis, Georgia Department of Transportation
Joe Gorman, Michigan Department of Transportation
Jason Graves, DENSO International America, Inc.
Ahmad Jawad, Commission of Oakland (RCOC)
Aravind Kailas, Volvo Group
John Kenney, Toyota Info Tech Labs
Tim McCall, Eberle Design, Inc. & Reno A&E
Dave Miller, Siemens
Ehsan Moradi Pari, Honda
Chris Poe, Mixon Hill
Faisal Saleem, Maricopa County Department of Transportation
Walt Townsend, Applied Information, Inc.
Joanna Wadsworth, City of Las Vegas

Subject Matter Experts (SMEs)

Justin Anderson, Noblis
Sue Bai, Honda
Ralph Boaz, Pillar Consulting
Wolfgang Buckel, Siemens
Patrick Chan, ConSysTec
Bronwen Crowe, ConSysTec
Deborah Curtis, USDOT
Zhitong Huang, Leidos
Manny Insignares, ConSysTec
Ed Leslie, Leidos
Jay Parikh, CAMP
Robert Rausch, TransCore
Steve Sill, USDOT
Chris Stanley, Leidos
Alan Toppen, Kimley-Horn
Michaela Vanderveen, Still Waters Consulting Inc.

Copyright Notice

NOTICE

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

NEMA, AASHTO, ITE AND THEIR SUPPLIERS DO NOT WARRANT THE PERFORMANCE OR RESULTS YOU MAY OBTAIN BY USING THESE MATERIALS. NEMA, AASHTO, ITE AND THEIR SUPPLIERS MAKE NO WARRANTIES, EXPRESSED OR IMPLIED, AS TO NON-INFRINGEMENT OF THIRD-PARTY RIGHTS, MERCHANTABILITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. IN NO EVENT WILL NEMA, AASHTO, ITE 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 A NEMA, AASHTO, OR ITE 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 exclusion of implied warranties, so the above limitations may not apply to you.

Use of these materials does not constitute an endorsement or affiliation by or between NEMA, AASHTO, or ITE, and you, your company, or your products and services.

If you are not willing to accept the foregoing restrictions, you should immediately return these materials.

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. NEMA, AASHTO and ITE standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest in the topic covered by this publication. While NEMA, AASHTO and ITE 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. NEMA, AASHTO or ITE 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. NEMA, AASHTO and ITE 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. NEMA, AASHTO and ITE 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, NEMA, AASHTO or ITE are not undertaking to render professional or other services for or on behalf of any person or entity, nor are they 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.

NEMA, AASHTO and ITE have no power, nor do they undertake to police or enforce compliance with the contents of this document. NEMA, AASHTO and ITE 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 NEMA, AASHTO or ITE and is solely the responsibility of the certifier or maker of the statement.

Additional Contributors and Reviewers

In addition to the SDOS, Co-Chairs, WG Members and SMEs, there were many others that contributed to the development of this standard and their input and assistance was critical to the final product. The following list includes those volunteers and others who gave their time to help both the consultant and the committee ensure that the resulting standard met their needs. The following is a more complete list of those who volunteered their time and travel to contribute to the input and review during the development of this standard:

Tony Ahmad, RS&H
Jim Alfred, Blackberry Ltd
Hassen Alwalie, Danlaw, Inc.
Auref Aslami, NCDOT
Kingsley Azubike, FHWA
Sue Bai, Honda
Rob Baily, Kapsch
Krishna Bandi, Ford Motor Company
Steve Bowles, 360 Network Solutions
Kevin Chan, Minnesota DOT
Alan Clelland, DKS and Associates
Matt D'Angelo, Gresham Smith
Julie Evans, RS&H
Chuck Felice, Utah DOT
Robert Fijol, FHWA
Ed Fok, FHWA
Mackenzie Francisco
Anthony Gasiorowski, WSP
Hideki Hada, Toyota Motor
Mohammed Hadi, FIU
Jacob Harel, Harman
Terry Haukom, Minnesota DOT
Nick Hegemier, DriveOhio
Craig Hinners, Intsignia
Matthew Huerta
Michael Ippoliti, Volvo Group
Haydar Issa, Transport Canada
Peter Jager, Utah DOT
Steve Johnson, HNTB
Mostafa Kassem, Danlaw, Inc.
Dmitri Khijniak, Parsons Transportation Group
Minseok Kim
Thomas M Kurihara, TKstds Management
AJ Lahiri, ConSysTec
Mike Lockerman, DENSO
Israel Lopez, Triunity, Inc.
Mack Martinez, Ford Motor
Jim Misener, Qualcomm Technologies, Inc.
Steve Misgen
Lee Mixon, Mixon Hill
Nadereh Moini, New Jersey Sports & Exposition Authority
Linda Nana, Noblis
Iouri Nemirovski, Siemens
Whitney Nottage, Q-Free / Intelight
Steve Orens, Volvo
Jonathan Parent, Transport Canada
Frank Perry, WSP
Christopher Poe, Mixon Hill, Inc.
Eric Raamot, Econolite
Pierre Rasoldier, Transport Canada
Randy Roebuck, OmniAir
Jesus Ruiz, McCain Inc.
Ted Sadler, Integral Blue
Robert Saylor, City of Plano, TX
Mike Schagrin, McCain, Inc.
Ed Seymour, Texas A&M Transportation Institute
Kellen Shain, Noblis
Suzanne Sloan, USDOT Volpe Center
Doug Spencer, Oregon DOT
Michael Stelts, Panasonic
John Thai, City of Anaheim
Danyang Tian, Honda
Jimmy Upton, Information Security
Drew Van Duren, Qualcomm Technologies, Inc.
Kevin Vitta, ITS America
Ivan Vukovic, Ford Motors
April Wire, Maricopa County DOT
Jingcheng Wu, HDR
Ken Yang, AECOM
Seora Yun
Kun Zhou, UC Berkeley PATH Program

Document History

Filename	Date	Author	Notes
RSU_Std_v01_SDD_v0117	05/24/21	Chan	RS Draft distributed to AASHTO, ITE, and NEMA for review/acceptance per organization's procedures.
RSU_Std_v01_SDD_v0116a	05/17/21	Crowe	Final updates from T. Kurihara
RSU_Std_v01_SDD_v0116	04/28/21	Crowe	Final security updates from D. Van Duren and M. Vanderveen
RSU_Std_v01_SDD_v0115e	04/22/21	Chan	Final revisions from Chan, Eisenhart. QA. For SME Review
RSU_Std_v01_SDD_v0115d	04/20/21	Crowe	Final revisions including input from Jimmy Upton, Justin McNew, Patrick Chan and Blaine Leonard.
RSU_Std_v01_SDD_v0115c	04/08/21	Crowe	Formatting changes
RSU_Std_v01_SDD_v0115b	04/06/21	Chan	Includes changes from SME meetings
RSU_Std_v01_SDD_v0115a_210331	03/31/21	McNew/ Crowe	Additional updates from Justin McNew and Michaela Vanderveen.
RSU_Std_v01_SDD_v0115a_210325	03/25/21	Chan	Additional UCD comments.
RSU_Std_v01_SDD_v0115a_210315	03/15/21	Crowe	Re-formatting NRTM; updates based on comments received on RSU UCD.
RSU_Std_v01_SDD_v0115	01/28/21	Crowe	Updated Cover Pages, Copyright Notice, Foreword for User Comment Draft
RSU_Std_v01_SDD_v0114d	01/22/21	Chan	Final Submission - SDD
RSU_Std_v01_SDD_v0114c	01/19/21	Crowe	Final updates based on comments from M. Vanderveen, J. Anderson, W. Buckel, Z. Huang, and R. Boaz.
RSU_Std_v01_SDD_v0114b	12/21/20	Chan	Submission for comments.
RSU_Std_v01_SDD_v0114a	12/21/20	Chan	Final updates
RSU_Std_v01_SDD_v0114	12/14/20	Crowe	Includes updates based on comments received during SDD Walkthrough.
RSU_Std_v01_SDD_v0113h	11/18/20	Chan	Draft SDD Document-Submittal
RSU_Std_v01_SDD_v0113g	11/17/20	Chan	Draft SDD Document-internal
RSU_Std_v01_SDD_v0113f	11/4/20	Chan	Includes WB comments. For WB review.
RSU_Std_v01_SDD_v0113e	11/2/20	Chan	Post SME meeting
RSU_Std_v01_SDD_v0113d	10/29/20	Chan	To WB for comments.
RSU_Std_v01_SDD_v0113c	10/27/20	Chan, Crowe	Added design section and updated RTM.
RSU_Std_v01_SDD_v0113b	10/13/20	Chan	Post SME meeting
RSU_Std_v01_SDD_v0113a	10/13/20	Chan	Includes WB comments
RSU_Std_v01_SDD_v0113	10/13/20	Chan	Outlines the SDD
RSU_Std_v01_FReqs_v0112	10/2/20	Chan, Crowe	Incorporates comments from comment period. Corrects the PICS
RSU_Std_v01_FReqs_v0111	9/15/20	Chan	Includes M. Vanderveen comments.
RSU_Std_v01_FReqs_v0110_200911	9/11/20	Crowe, Chan	Inputs from the FR Walkthrough
RSU_Std_v01_FReqs_v0109-D3	8/27/20	Chan	Markups during the FR Walkthrough.
RSU_Std_v01_FReqs_v0108	8/11/20	Chan	Submittal to RSU WG.
RSU_Std_v01_FReqs_v0107_200811e	8/11/20	Crowe	NRTM Inputs and updated Figure 1 from RB.
RSU_Std_v01_FReqs_v0107_200810e	08/10/20	Chan	SME Meeting Changes

Filename	Date	Author	Notes
RSU_Std_v01_FReqs_v0107_200810d	08/10/20	Crowe	Input of Requirements from JA, RB, and JP.
RSU_Std_v01_FReqs_v0107_200804d	08/05/20	Crowe/ Chan	Input of Requirements from JM.
RSU_Std_v01_FReqs_v0107_200803d	08/03/20	Chan	SME Meeting changes
RSU_Std_v01_FReqs_v0107_200730c	07/30/20	Chan	Chan updates
RSU_Std_v01_FReqs_v0107_200720b	07/27/20	Chan	SME Meeting changes
RSU_Std_v01_FReqs_v0107_200720a	07/20/20	Crowe/ Chan	SME Meeting changes
RSU_Std_v01_FReqs_v0107_200720	07/20/20	Crowe/ Chan	Inserted NRTM and Requirements from WB, PC, JA, and RB.
RSU_Std_v01_FReqs_v0107_200716	07/16/20	Crowe/ Chan	Inserted Section 3 from RB.
RSU_Std_v01_ConOps_v0106_200712	07/02/20	Boaz	Changes made based on adjudication of comments received on ConOps v01.05.
RSU_Std_v01_ConOps_v0105_200605	06/05/20	Boaz	Changes based on decisions made during the ConOps Walkthrough. Document distributed to WG for review and comment.
RSU_Std_v01_ConOps_v0104_200528	05/28/20	Boaz	Name change and typo correction. Version used for ConOps Walkthrough June 1-2, 2020.
RSU_Std_v5_ConOps_v0104_200524	05/24/20	Boaz	Edits post WG Mtng 05/22/20.
RSU_Std_v5_ConOps_v0103_200521	05/21/20	Boaz	Edits post WG Mtng 05/20/20.
RSU_Std_v5_ConOps_200520a	05/20/20	Boaz	Edits during WG Mtng 05/20/20.
RSU_Std_v5_ConOps_200520	05/20/20	Boaz	Complete ConOps including architectural diagrams prior to WG Mtng 05/20/20.
RSU_Std_v5_ConOps_200519_JP_RR	05/20/20	Chan	Combined edits from JP, RR
RSU_Std_v5_ConOps_200519	05/19/20	Boaz	Edits from PXC, WB, JPM, JA, and RB
RSU_Combined ConOps Contributions-200515edits.docx	05/15/20	Chan	Edits from 5/15/20 SME meeting
RSU_Combined ConOps Contributions-200513edits+JPM to JP.docx	05/15/20	Crowe	Additional edits from JPM and JA.
RSU_Combined ConOps Contributions-200513edits.docx	05/13/20	Chan	Edits from 5/13/20 SME meeting
RSU_Combined ConOps Contributions.docx	05/13/20	Crowe	Combined initial contributions

Table of Contents

Table of Figures

List of Tables

<This page intentionally left blank.>

Section 1
General Information [Informative]

1.1 Scope

This document establishes a non-proprietary, industry-consensus Roadside Unit (RSU) Standard. An RSU is a transportation infrastructure communications device that is a part of a Cooperative Intelligent Transportation Systems (C-ITS) transportation environment. The goal of such an environment is to reduce the number of fatalities and injuries on roadways, improve mobility, and reduce environmental impacts of transportation systems. Commonly known as the Connected Vehicle (CV) environment in the United States, it includes both connected human-driven vehicles and connected automated vehicles (CAVs). The terms Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) are used to reflect the exchanges of messages within the CV environment. The vision for this technology has expanded to include all types of travelers including pedestrians, cyclists, multimodal travelers, and other vulnerable road users, and is referred to as Vehicle-to-Everything (V2X) technology and V2X communications.

Services to the traveler are carried out through on-board units (OBUs) that are installed in vehicles or mobile units (MUs) that are used for other modes of transportation. A vehicle can receive traffic signal timing information and warn the driver of a potential red-light violation. A bus can receive traffic signal priority. A pedestrian can activate a crosswalk without the push of a button. These examples require an interface between the OBUs/MUs and the transportation infrastructure. An RSU provides this interface by connecting wirelessly to OBUs/MUs and through Ethernet connections to traffic control devices, traffic management systems (TMSs) and back-office systems. The RSU communicates wirelessly with OBUs/MUs via its V2X interface.

The United States Department of Transportation (USDOT) has made significant previous investments in defining the user needs, requirements, and design elements of RSUs through FHWA-JPO-17-589, *Dedicated Short-Range Communications Roadside Unit Specifications v4.1* (see Section 1.2.2, also referred to as RSU Specifications 4.1) and the development of National Transportation Communications for ITS Protocol (NTCIP) 1218 v01 Object Definitions for Roadside Units (see Section 1.2.1). Additionally, there are multiple deployment efforts where real-world experience with RSUs is being gained, such as the USDOT's Connected Vehicle Pilot programs and Signal Phase and Timing (SPaT) Challenge projects. This standard has been developed by incorporating knowledge gained from these previous documents and pilot programs, and using a systems engineering (SE) approach with multidisciplinary stakeholders.

1.2 References

1.2.1 Normative References

Normative references contain provisions that, through reference in this text, constitute provisions of this RSU Standard. Other references in this document 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 using this RSU Standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed.

Table 1. Normative References

Identifier	Title
3GPP TS 23.285	Architecture Enhancements for V2X Services, 3GPP.
CAMP CV Pilots Documentation	CAMP CV Pilots Documentation material. https://wiki.campllc.org/display/SCP/SCMS+CV+Pilots+Documentation **NOTE - TO BE UPDATED USING A USDOT LINK**

Identifier	Title
CAMP Platform Security Document	"Hardware, Software and OS Security Requirements", CAMP, April 11, 2018. https://wiki.campllc.org/display/CPD/CAMP+Public+Documents+Home?preview=%2F143491424%2F143491426%2FHardware+Software+and+OS+Security+Requirements-v106-20180411_1423.pdf **NOTE - TO BE UPDATED USING A USDOT LINK**
IEC 60529	Degrees Of protection provided by enclosures (IP Code), International Electrotechnical Commission, Ed. 2.2, 2013.
IEC 61000-4-2:2008	Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test, International Electrotechnical Commission, Ed. 2.0, 2008.
IEC 61000-4-4:2012	Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test, International Electrotechnical Commission, Ed. 3.0, 2012.
IEC 61000-4-5:2017	Electromagnetic compatibility (EMC) - Part 4-5: Testing and measurement techniques - Surge immunity test, International Electrotechnical Commission, Ed. 3.1, 2017.
IEC 61000-6-2:2016	Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity standard for industrial environments, International Electrotechnical Commission, Ed. 3.0, 2016.
IEC 62368-1:2018	Audio/video, information and communication technology equipment - Part 1: Safety requirements, International Electrotechnical Commission, Ed 3.0, 2018.
IEEE Std 802.3™-2018	IEEE Standard for Ethernet, IEEE, 2018.
IEEE Std 802.11™-2020	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, IEEE, 2020.
IEEE Std 1609.2™-2016	IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages, IEEE, 2016, with Amendments IEEE 1609.2a-2017 and IEEE 1609.2b-2019.
IEEE Std 1609.2b™-2019	IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages - Amendment 2--PDU Functional Types and Encryption Key Management, IEEE, 2019.
IEEE Std 1609.2.1™-2020	IEEE Standard for Wireless Access in Vehicular Environments--Certificate Management Interfaces for End-Entities, IEEE, 2020.
IEEE Std 1609.3™-2020	IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Networking Services, IEEE, 2020.
IEEE Std 1609.4™-2016	IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation, IEEE, 2016.
IETF RFC 5905	Network Time Protocol Version 4: Protocol and Algorithms Specification, Internet Engineering Task Force (IETF), June 2010.
IETF RFC 6146	Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers, Internet Engineering Task Force (IETF), April 2011.
IETF RFC 8446	The Transport Layer Security (TLS) Protocol Version 1.3, Internet Engineering Task Force (IETF), August 2018.
ITU-R TF.460-6	Standard-frequency and time-signal emission, International Telecommunications Union, 2002.
MIL-STD-810H	Environmental Engineering Considerations and Laboratory Tests, Department of Defense, Test Method Standard, 31 January 2019.
NEMA TS 2-2016	NEMA Standards Publication TS 2-2016, Traffic Controller Assemblies with NTCIP Requirements, Version 3.07, NEMA, 2016.
NEMA TS 10-2020	Connected Vehicle Infrastructure - Roadside Equipment, NEMA, March 3, 2021.

Identifier	Title
NIST FIPS 140-2	Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, March 22, 2019. https://doi.org/10.6028/NIST.FIPS.140-2
NTCIP 1218 v01	Object Definitions for Roadside Units (RSUs), AASHTO / ITE / NEMA, published September 2020.
SAE J3101_202002	Hardware Protected Security for Ground Vehicles, SAE International, 2020
TIA-607-D	Generic Telecommunications Bonding and Grounding (Earthing) for Customer Premises, Revision D, Telecommunications Industry Association (TIA), July 2019.
V2I Hub ICD	Integrated Vehicle-to-Infrastructure Prototype (IVP), V2I Hub Interface Control Document (ICD) - Final Report, FHWA JPO, March 2017. [https://usdot-carma.atlassian.net/l/c/qznaJ0DB]

1.2.2 Other References

The following documents and standards may provide the reader with a more complete understanding of RSU-related equipment and communications. However, these documents do not contain direct provisions that are required by the RSU Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on the RSU Standard are encouraged to investigate the possibility of applying the most recent editions of the standard listed.

Table 2. Other References

Identifier	Title
ARC-IT	Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT), USDOT.
ATC 5201 v06A	Advanced Transportation Controller (ATC) Standard Version 06A, ATC Joint Committee, July 2020.
ATC 5401 v02A	Application Programming Interface (API) Standard for the Advanced Transportation Controller (ATC) Version 02A, ATC Joint Committee, July 2020.
BS EN 50556:2018	Road traffic signal systems, British-Adopted European Standard, October 4, 2018.
CFR Title 47 – Telecommunication	Code of Federal Regulations, Title 47 – Telecommunication, Chapter 1 – Federal Communications Commission, Part 15 and Part 90 (Regulations Governing the Use of Frequencies in the 5850-5925 MHz Band).
CIS Controls Implementation Guide for Industrial Control Systems	CIS Controls Implementation Guide for Industrial Control Systems, Center for Internet Security, Version 7.1.
FHWA-JPO-17-589 (RSU Specification 4.1)	Dedicated Short-Range Communications Roadside Unit Specifications v4.1, USDOT, Saxton Transportation Operations Laboratory, published April 28, 2017. Note: Also referred to as RSU Specifications 4.1.
IEC 60068-2-64:2008	Environmental Testing - Part 2-64: Tests - Test Fh: Vibration, broadband random and guidance, International Electrotechnical Commission, Ed. 2.0, 2008.
IETF RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), Internet Engineering Task Force (IETF), December 2002.
IETF RFC 5246	The Transport Layer Security (TLS) Protocol Version 1.2, Internet Engineering Task Force (IETF), August 2008.
IETF RFC 5424	The Syslog Protocol, Internet Engineering Task Force (IETF), June 2010.

Identifier	Title
IETF RFC 5590	Transport Subsystem for the Simple Network Management Protocol (SNMP), Internet Engineering Task Force (IETF), June 2009.
IETF RFC 5591	Transport Security Model for the Simple Network Management Protocol (SNMP), Internet Engineering Task Force (IETF), June 2009.
IETF RFC 6353	Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP), Internet Engineering Task Force (IETF), June 2009.
ISO/IEC/IEEE 24765:2017	ISO/IEC/IEEE International Standard – Systems and Software Engineering – Vocabulary, 2017. https://pascal.computer.org/
ISO/TS 21177:2019	Intelligent transport systems - ITS station security services for secure session establishment and authentication between trusted devices. ISO, 2019.
LRFDLTS-1	AASHTO LRFD Specifications for Structural Supports for Highway Signs, Luminaires, and Traffic Signals, 1st Edition, 2015.
NIST FIPS PUB 197	Announcing the Advanced Encryption Standard (AES), National Institute of Standards and Technology (NIST), November 26, 2001. https://doi.org/10.6028/NIST.FIPS.197
NIST 800-63B	NIST Special Publication 80-63-3, Digital Identity Guidelines, National Institute of Standards and Technology (NIST), June 2017. https://doi.org/10.6028/NIST.SP.800-63B
NTCIP 1202 v03A	Object Definitions for Actuated Signal Controllers (ASC) Interface. AASHTO/ITE/NEMA, published May 2019.
SAE J2735_202007	V2X Communications Message Set Dictionary™, SAE International, 2020.
SAE J2945/3_202003	Requirements for Road Weather Applications, SAE International, 2020.
SAE J2945_201712	Dedicated Short Range Communication (DSRC) Systems Engineering Process Guidance for SAE J2945/X Documents and Common Design Concepts, SAE International, 2017.
SAE J3161	C-V2X Deployment Profiles, SAE International, 2021.
SCMS EE Certificate Rollover (Re-enrollment) Technical Standard v01	EE Certificate Rollover (Re-enrollment) Technical Standard, v1.0, SCMS Manager LLC, October 8, 2020; https://www.scmsmanager.org/wp-content/uploads/2020/10/SCMS-Manager-EE-Re-Enrollment-Technical-Specification-v1.0.pdf

1.2.3 Contact Information

1.2.3.1 3GPP Documents

Copies of 3GPP documents may be obtained electronically from:

http://www.3gpp.org/

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 Advanced Transportation Controller (ATC) Standards

Copies of Advanced Transportation Controller (ATC) Standards may be obtained electronically from:

https://www.ite.org/technical-resources/standards/

1.2.3.4 International Electrotechnical Commission (IEC)

International Electrotechnical Commission (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

1.2.3.5 IEEE

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

1.2.3.6 Internet Documents

Obtain Request for Comment (RFC) electronic documents from several repositories on the World Wide Web, or by “anonymous” File Transfer Protocol (FTP) with several hosts. Browse or FTP to:

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

1.2.3.7 International Telecommunications Union (ITU)

International Telecommunications Union (ITU) 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

1.2.3.8 National Transportation Communications for ITS Protocol (NTCIP)

Copies of NTCIP standards may be obtained from:

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

1.2.3.9 National Electrical Manufacturers Association (NEMA)

National Electrical Manufacturers Association (NEMA) 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/nema

1.2.3.10 SAE International

Copies of SAE International documents may be obtained from:

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

1.2.3.11 USDOT/FHWA

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 and Open Science Access Portal (ROSA P):

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

1.3 Terms

The following terms, definitions, acronyms, and abbreviations are used in this document.

Table 3. Terms

Term	Definition
Cellular Vehicle-to-Everything (C-V2X)	A V2X communications interface conforming to 3GPP TS 23.285.
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 Specifications 4.1 is based on 1/1/1970 while IEEE Std 1609.2™-2016 security is based on 1/1/2004 and needs to adjust for leap-year seconds.
Dedicated Short Range Communications (DSRC)	A V2X communications interface conforming to IEEE Std 802.11™:2012 (802.11p).
Hardware Security Module (HSM)	A secure hardware device used to store root certificates and private key pairs.
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).

Term	Definition
Interoperability	The ability of two or more systems or components to exchange information and use the information that has been exchanged (ISO/IEC/IEEE 24765-2017 International Standard – Systems and software engineering – Vocabulary).
Mobile Unit (MU)	A device used to wirelessly communicate with other devices for safety and mobility purposes carried by a pedestrian, bicyclist, work zone worker, or other traveler.
On-Board Unit (OBU)	A device used to wirelessly communicate with other devices for safety and mobility purposes installed in a vehicle as original equipment or as aftermarket equipment (sometimes referred to as an “aftermarket safety device (ASD)”.
Operator	A user of a traffic management system or back-office system. An operator may be located in a traffic management center, co-located with some other back-office system, or work with a system from a remote location.
Roadside Cabinet Electronics (RSCE)	These are the electronics necessary to physically integrate the V2X technology into an on-street enclosure. Typically, one used for a transportation field cabinet system but other enclosures are not excluded.
Roadside Equipment (RSE)	A broad term that includes the RSU and other ITS field equipment (includes traffic signal controllers).
Roadside Unit (RSU)	A transportation infrastructure communications device located on the roadside that provides V2X connectivity between OBUs/MUs and other parts of the transportation infrastructure including traffic control devices, traffic management systems, and back-office systems. Note: Devices that are not part of the transportation infrastructure, such as cellular base stations or satellites, are not RSUs.
Security Credential Management System (SCMS)	A Public Key Infrastructure (PKI) system with special features for the support of V2X communications; encompassing entities that issue IEEE Std 1609.2™-2016 digital certificates to vehicles and infrastructure nodes to support trustworthy communication.
Traffic Signal Controller (TSC)	A field hardened computing device that runs the application program(s) for a transportation field cabinet system. Historically, TSCs run a single application program. TSCs that conform to the ATC 5201 and ATC 5401 standards, use modern processors, a Linux operating system, and can run multiple application programs concurrently on a single controller unit.
Transportation Field Cabinet System (TFCS)	The on-street system used to perform various transportation applications. The most common applications are traffic signal control, ramp metering, and data collection.
Traveler	A motorist, pedestrian, cyclist, or other multimodal user of the transportation infrastructure.
Vulnerable Road User (VRU)	A term applied to those most at risk in traffic, i.e., those unprotected by an outside shield. VRUs are pedestrians (especially children, seniors and people with disabilities), bicyclists, and motor cyclists.

Term	Definition
V2X Interface	A logical component of the RSU representing the wireless interface between the RSU and OBUs/MUs.

1.4 Abbreviations

The abbreviations and acronyms used in this document are defined below.

Table 4. Abbreviations

3GPP	3rd Generation Partnership Project
AASHTO	American Association of State Highway Transportation Officials
API	Application Programming Interface
ARC-IT	Architecture Reference for Cooperative and Intelligent Transportation
ASC	Actuated Signal Control
ATC	Advanced Transportation Controller
BSM	Basic Safety Message
C-ITS	Cooperative Intelligent Transportation Systems
CA	Certificate Authority
CCH	Control Channel
CFR	Code of Federal Regulations
ConOps	Concept of Operations
CORS	Continuously Operating Reference Station
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CV	Connected Vehicle
C-V2X	Cellular Vehicle-to-Everything
CVRE	Connected Vehicles Roadside Equipment
CVRIA	Connected Vehicle Reference Implementation Architecture
DSRC	Dedicated Short Range Communications
ECA	Enrollment Certificate Authority
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESD	Electrostatic Discharge
FCC	Federal Communications Commission
FHWA	Federal Highway Administration
FIPS	Federal Information Processing Standards

FTP	File Transfer Protocol
FO	Functional Object
GMT	Greenwich Mean Time
GNSS	Global Navigation Satellite System
HSM	Hardware Security Module
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IOO	Infrastructure Owner Operator
IP	Internet Protocol
ISO	International Organization for Standardization
ISO/TS	ISO Technical Specifications
IT	Information Technology
ITE	Institute of Transportation Engineers
ITS	Intelligent Transportation Systems
JPO	USDOT ITS Joint Program Office
LCCF	Local Certificate Chain File
LPF	Local Policy File
MAP	Intersection Geometry Message
MCD	Millicandela
MU	Mobile Unit
NEMA	National Electrical Manufacturers Associations
NIST	National Institute of Standards and Technology
NTCIP	National Transportation Communications for ITS Protocol
NTP	Network Time Protocol
NTRIP	Network Transport of RTCM via Internet Protocol
OBU	On-Board Unit
OEM	Original Equipment Manufacturers
OTA	Over-The-Air
PICS	Protocol implementation Conformance Statement
PoE	Power-over-Ethernet
PoE+	Power-over-Ethernet Plus
PSID	Provider Service Identifier
RFC	Request for Comment
RA	Registration Authority

RF	Radio Frequency
RFI	Radio Frequency Interference
ROSA P	Repository and Open Science Access Portal
RSCE	Roadside Cabinet Electronics
RSE	Roadside Equipment
RSM	Road Safety Message
RSPA	Roadside Processing Application
RSU	Roadside Unit
RSU WI	Roadside Unit Wireless Interfaces
RWM	Road Weather Message
SAE	SAE International (formerly Society of Automotive Engineers)
SCA	Signal Control Application
SCH	Service Channel
SCMS	Security Credential Management System
SDO	Standards Development Organizations
SE	Systems Engineering
SNMP	Simple Network Management Protocol
SPaT	Signal Phase and Timing or Signal Phase and Timing Message
SRM	Signal Request Message
SSM	Signal Status Message
SSP	Service Specific Permissions
STA	Station
TFCS	Transportation Field Cabinet System
TIM	Traveler Information Message
TLS	Transport Layer Security
TMC	Traffic Management Center
TMS	Traffic Management System
TSC	Traffic Signal Controller
TSCBM	Traffic Signal Controller Broadcast Message
US	United States
USDOT	United States Department of Transportation
UTC	Coordinated Universal Time (also called “Common Universal Time”)
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle

V2X	Vehicle-to-Everything
VPN	Virtual Private Network
VRU	Vulnerable Road User
WAVE	Wireless Access in Vehicular Environment
WRA	WAVE Routing Advertisement
WSA	WAVE Service Advertisement
WSMP	WAVE Short Message Protocol

Section 2
Concept of Operations [Normative]

2.1 Tutorial [Informative]

In systems engineering, the different stages of the definition and design process are captured in documents suitable for the stage of development of the system (or device). A concept of operations (ConOps) is a document that describes characteristics for the proposed system from the user's perspective. The goal is to have a common understanding between the users of the system and those that develop requirements for the system. User needs for the system are identified by a collaboration of a broad base of stakeholders and some are drawn from existing documents. Each user need is captured in the ConOps in a formal manner along with the rationale which justifies the inclusion of the need and may also provide other clarifying information so that the user need is understood in subsequent stages of development.

This ConOps has been prepared as part of the development of an RSU Standard. The terms “Normative” and “Informative” are used to distinguish parts of this ConOps that must be conformed to (Normative) and those that are there for informational purposes (Informative). It is possible for a section to be identified as Normative but have subsections that are identified as Informative. If a section is identified as Normative, then all of its subsections are to be considered Normative unless identified otherwise.

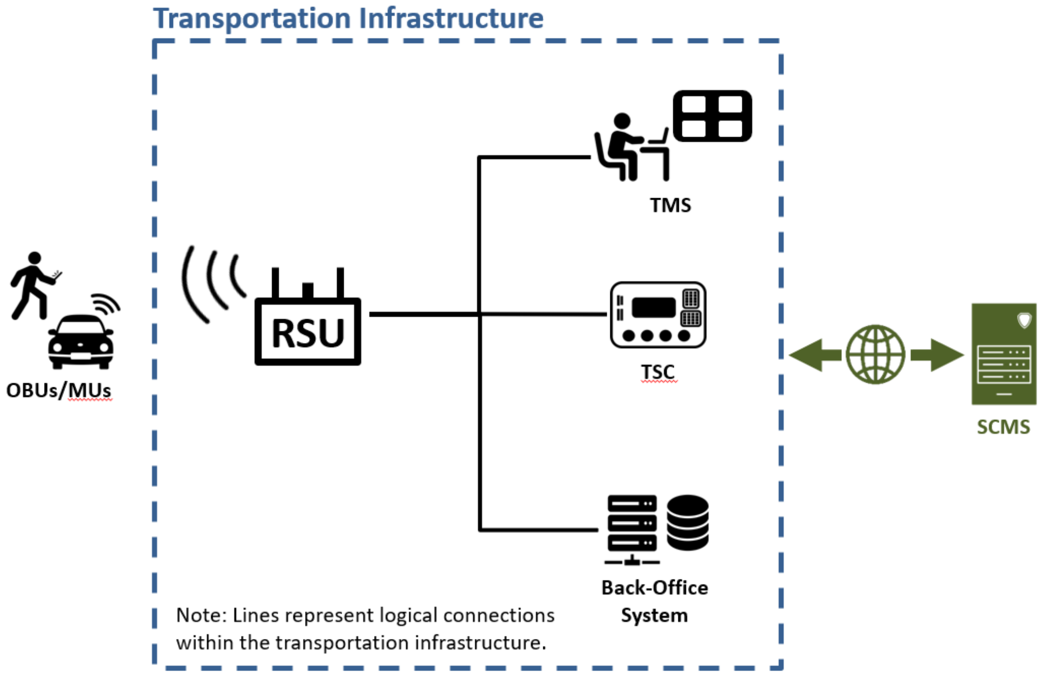
The remaining sections of this ConOps are as follows:

- **Section 2.2 Current Situation and Problem Statement [Informative].** This section describes the current situation and issues that have led to the need for an RSU Standard.
- **Section 2.3 Operational and Physical Architecture [Informative].** This section describes the operational architectures for RSUs that are known to exist.
- **Section 2.4 RSU Logical Architecture [Informative].** This section describes the logical architecture of an RSU.
- **Section 2.5 Needs [Normative].** This section identifies the user needs for the RSU.
- **Section 2.6 Operational Policies and Constraints [Normative].** This section identifies any operational policies and constraints.
- **Section 2.7 Relationship to ARC-IT [Informative].** This section describes how the RSU fits into the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT).

2.2 Current Situation and Problem Statement [Informative]

Vehicle-to-everything (V2X) technology has been designed to help mitigate various transportation related issues (e.g., crashes, congestion, delays, pollution). Using V2X communications, OBUs/MUs and RSUs can exchange critical information to improve safety and mobility for vehicles, vulnerable road users (e.g., cyclists, pedestrians, motorcycles), and other road users. By receiving real-time infrastructure information (e.g., traffic signal phasing and timing, details about the intersection geometry), road users can more efficiently travel on roadways with reduced delays, improved fuel efficiency, and reduced emissions. In addition, after obtaining real-time status information from OBUs/MUs, active or proactive traffic management strategies can be implemented by operators in traffic management centers (TMCs) in order to reduce congestion and improve mobility.

Figure 1 shows the high-level structure of a V2X system. Roadside units (RSUs) are the key element of the system since they exchange data with OBUs/MUs and other infrastructure elements. RSUs can receive messages from OBUs/MUs and forward these messages to transportation infrastructure elements (e.g., traffic management systems, traffic signal controllers (TSCs), back-office data storage) to provide information about real-time traffic conditions. Similarly, RSUs broadcast real-time critical infrastructure information, such as Signal Phase and Timing (SPaT), information about the intersection’s geometry (MAP), and Traveler Information (TIM), over the air to OBUs/MUs to inform travelers of current and upcoming traffic management strategies, conditions, and incidents. Any transportation infrastructure device capable of signing messages has a direct connection to the SCMS (Security Credentials Management System). Although Figure 1 shows that the OBUs/MUs communicate to the SCMS via the RSU, OBUs/MUs may have their own connection to the SCMS e.g., via cellular or Wi-Fi or other wireless technologies.



Note: Lines represent logical connections within the transportation infrastructure.

Figure 1. V2X System

Because of the crucial role of RSUs in the V2X communications, its functionalities and performance have significant impacts on the safety and operation of the entire V2X ecosystem, including cooperative automation systems that may use V2X. A growing number of transportation agencies have started to invest resources to include V2X technology in their transportation systems by deploying RSUs, since V2X technology brings significant benefits to their operations. Transportation agencies may use different models or different manufacturers of RSUs in order to deploy V2X technology. For this reason, interoperability of RSUs becomes critical for maximizing the benefits of V2X technology regionally and nationally. The goal of this standard is to facilitate V2X interoperability by defining the required functionality to be provided by RSU manufacturers.

In 2017, the USDOT published RSU Specifications 4.1 which incorporated input from industry, including device vendors, users, and early deployers, to define the minimum performance requirements of RSUs. It specified power requirements, environmental requirements, physical requirements, functional requirements, behavioral requirements, performance requirements, and interface requirements of RSUs. RSU Specifications 4.1 required the use of Simple Network Management Protocol (SNMP) Version 3 (SNMPv3) communications to configure and operate RSUs, as well as various health and status monitoring features, to support the secure management of RSUs network-wide.

V2X technology has developed rapidly in the last three years and the functionality defined in RSU Specifications 4.1 needs to evolve to meet current needs. New standards have been developed, including NTCIP 1218 v01, which defines an RSU management interface and NEMA TS 10-2020, which describes desired operational situations for RSU standards. This comprehensive RSU Standard addresses current needs by:

- Helping IOOs procure RSUs that are conformant with national standards and that address their use cases;
- Facilitating RSU compatibility and interoperability with OBUs and MUs from different manufacturers;
- Facilitating RSU compatibility and interoperability with traffic control devices from different manufacturers;
- Facilitating the interchangeability of RSUs from different manufacturers;
- Providing for the use of emerging wireless technologies that may be introduced in the RSU's service life;
- Providing security for the RSU and its communication interfaces; and
- Defining the functionality of RSUs that will exchange standardized V2X messages to improve safety and mobility.

This standard satisfies the needs summarized above by defining functional requirements, behavioral requirements, performance requirements, and interface requirements in order to support deployment of V2X technology in North America.

2.3 Operational and Physical Architecture [Informative]

This section contains figures representing examples of the operational architectures and physical layouts for RSUs. There are different RSU mounting options and configurations based on the physical layout of the intersection and systems. When deploying RSUs, some of the factors to consider are:

a) the radio line of sight for optimal placement of antennas;
b) distance limitations between the RSU and the Roadside Cabinet Electronics (RSCE) due to Power over Ethernet (PoE) connections commonly used;
c) environmental factors;
d) the capabilities of the TCS;
e) recommendations from RSU, OBU, and MU manufacturers;
f) GNSS satellite visibility; and
g) serviceability.

There may be operational architectures not shown. The elements of these architectures are described below.

- **Roadside Unit (RSU)** – Performs the data exchange between OBUs/MUs and infrastructure elements. An RSU may be a single device or the RSU may be distributed between different devices to meet the operational needs of the IOO.
- **Roadside Unit Wireless Interfaces (RSU WI)** – Part of a distributed RSU architecture where the unit mounted on a pole or mast arm only contains the electronics necessary for the radio interfaces of the RSU. The message processing function of the RSU is performed in a different device.
- **Transportation Field Cabinet** – Contains the Transportation Field Cabinet System (TFCS) used to perform on-street transportation applications. The most common applications are intersection control, ramp metering, and data collection. The most significant device in a TFCS is the TSC.
- **Traffic Signal Controller (TSC)** – A field hardened computing device that runs the application program(s) for a transportation field cabinet system. Historically, TSCs run a single application program. TSCs that conform to the ATC 5201 and ATC 5401 standards, use modern processors, a Linux operating system, and can run multiple application programs concurrently on a single TSC unit.
- **Signal Control Application (SCA)** – The application program that runs in a TSC to perform the function of operating an intersection.
- **Roadside Processing Application (RSPA)** – The application program that runs in an RSU, TSC or other device to perform the message processing function of an RSU. Unless stated otherwise, the RSPA is a part of the RSU.

- **Roadside Cabinet Electronics (RSCE)** – These are the electronics necessary to physically integrate the RSU into the TFCS.
- **Traffic Management System (TMS)** – The system used by traffic operations staff to configure, control, monitor, and collect data from the TFCS in order to manage traffic.
- **Back-Office System** – Separate system for storage and processing of connected vehicle and device data.
- **On-Board Unit / Mobile Unit (OBU/MU)** – Perform the data exchange between the RSU and non-infrastructure devices. On-Board Units may be installed in motor vehicles (integrated or aftermarket) and MUs may be integrated with cellular phones or otherwise be carried by pedestrians, cyclists, other travelers, or workers in the roadway.

Figure 2 illustrates an RSU as a single device mounted on a mast arm. Typically, the RSU connects to the RSCE using Ethernet. Other interfaces may also be supported. The RSCE connects to the TSC using a wired connection (e.g., Ethernet).

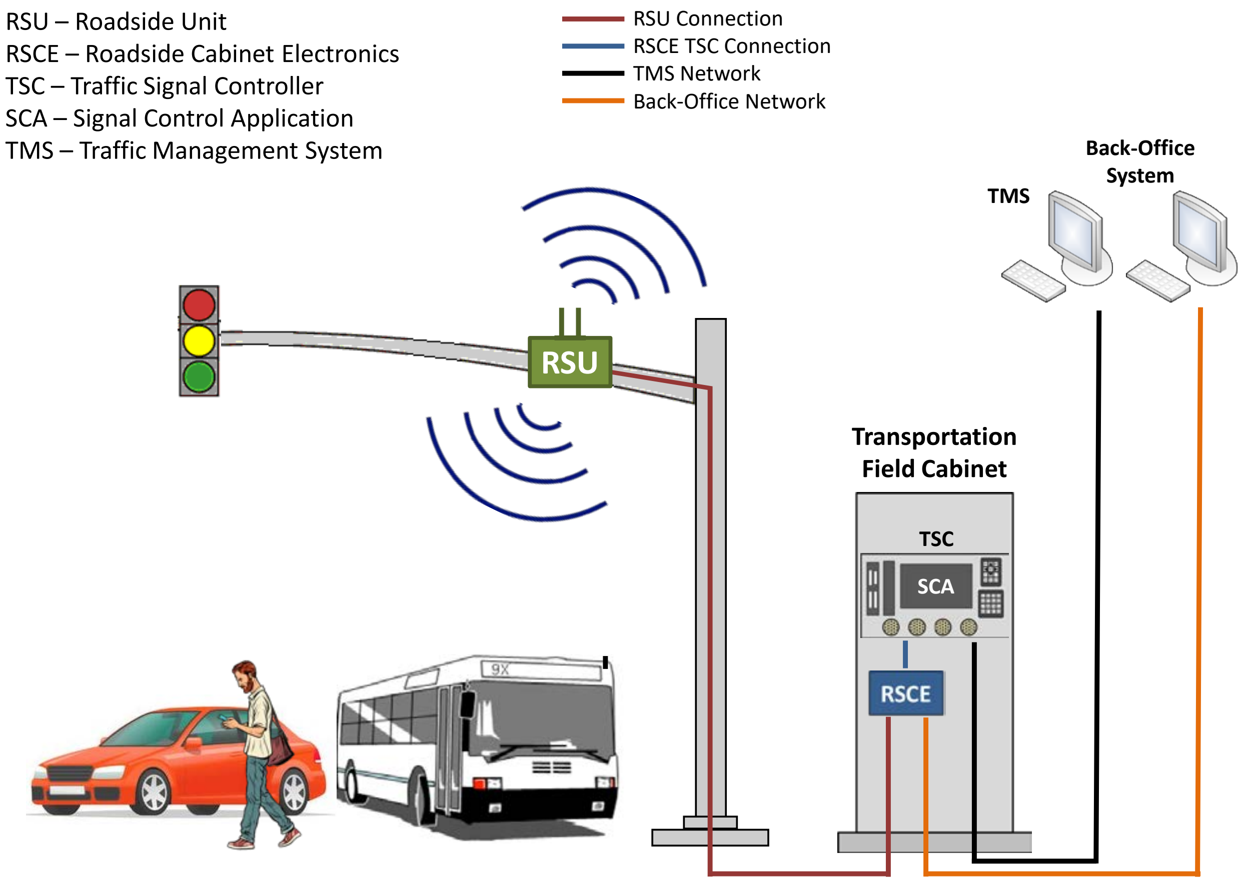

RSU – Roadside Unit
RSCE – Roadside Cabinet Electronics
TSC – Traffic Signal Controller
SCA – Signal Control Application
TMS – Traffic Management System
RSU Connection
RSCE TSC Connection
TMS Network
Back-Office Network
Back-Office System
TMS
RSU
Transportation Field Cabinet
TSC
SCA
RSCE
9X

Figure 2. Example of an RSU mounted on a mast arm of a traffic signal

Figure 3 illustrates an RSU as a device mounted on a pole or a mast arm with the antennas mounted separately on a mast arm. This is done when weight or wind are concerns for a particular mast arm. Typically, the RSU connects to the RSCE using Ethernet. Other interfaces may also be supported. The RSCE connects to the TSC using a wired connection (e.g., Ethernet).

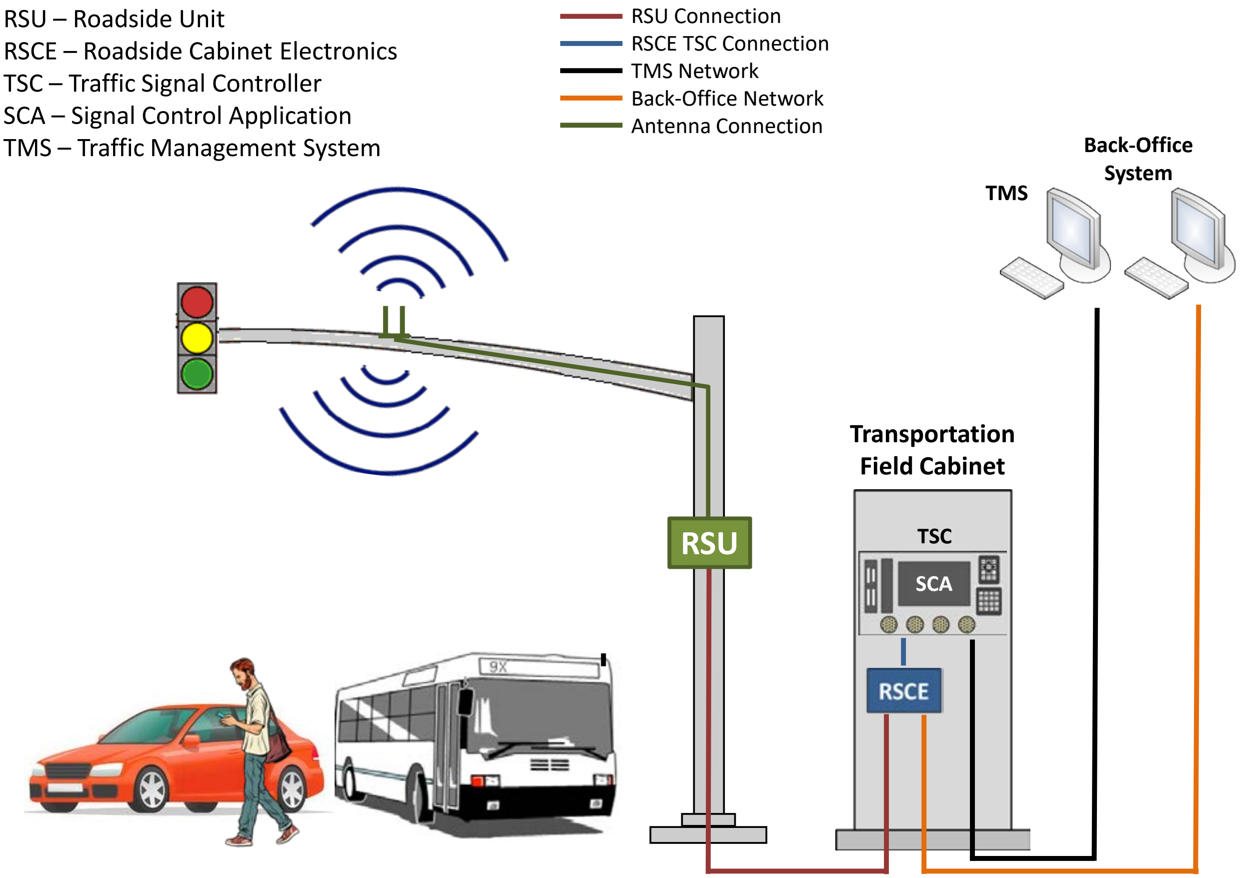

RSU – Roadside Unit
RSCE – Roadside Cabinet Electronics
TSC – Traffic Signal Controller
SCA – Signal Control Application
TMS – Traffic Management System
RSU Connection
RSCE TSC Connection
TMS Network
Back-Office Network
Antenna Connection
Back-Office System
TMS
Transportation Field Cabinet
TSC
SCA
RSCE
RSU
9X

Figure 3. Example of an RSU mounted on a pole with antennas mounted on the mast arm

Figure 4 illustrates an RSU mounted along a roadway where it is not associated with an intersection. This architecture may be used on freeways for data collection, traveler information or other message exchanges. In this example, the RSU as a device mounted on the mast arm of a streetlight with the antennas mounted separately on a mast arm. Typically, the RSU connects to the RSCE using Ethernet. Other interfaces may also be supported. The RSCE makes the connection to the back-office network. No TFCS or TSC is used.

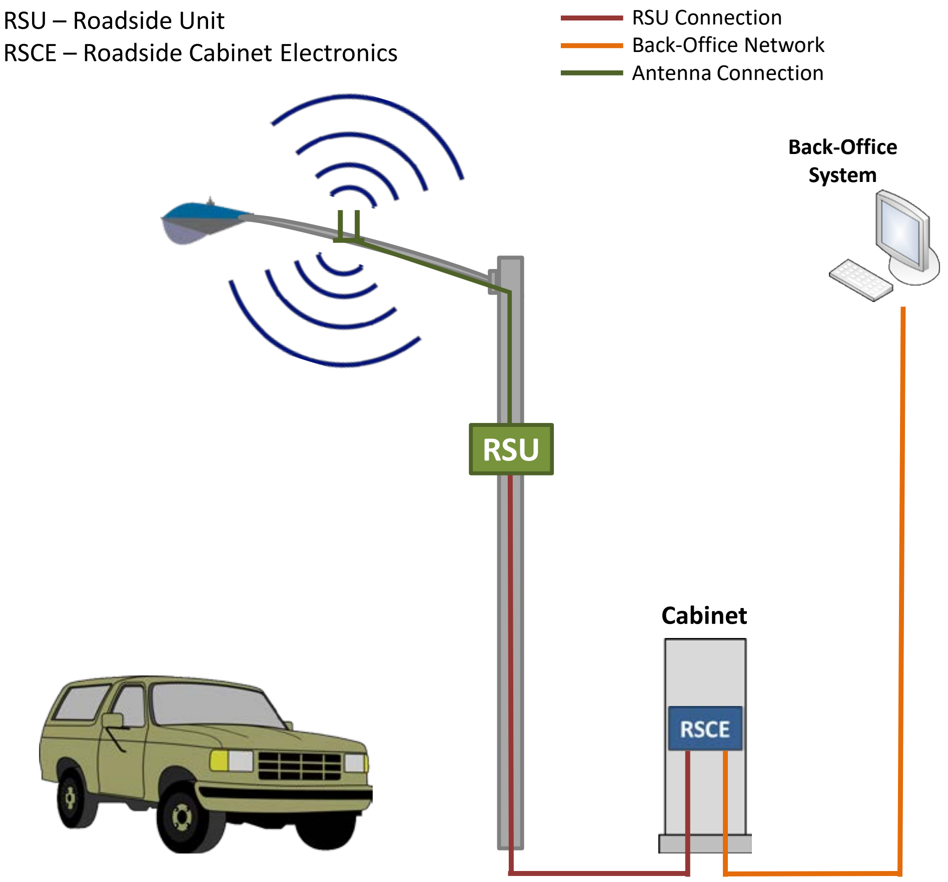


Figure 4. Example of an RSU mounted along a roadway (non-intersection installation).

2.4 RSU Logical Architecture [Informative]

Figure 5 show the logical architecture of an RSU with its elements and connections that correspond to the operational and physical architectures found in the Section 2.3. In addition to the elements listed in Section 2.3 the elements described below are used in the logical architecture.

- **GNSS Satellite** – Transmits positioning and timing data to GNSS receivers.
- **V2X Radio (and Antenna)** – Transmits and receives wireless messages with the OBUs/MUs.
- **GNSS Receiver (and Antenna)** – Used to receive GNSS positioning information and time.
- **Hardware Security Module** - A secure hardware device used to store root certificates and private key pairs.

Figure 5 illustrates the logical architecture for the operational architecture and physical layout shown in Figure 2 and Figure 3. In this configuration, the antennas are mounted separately from the unit.

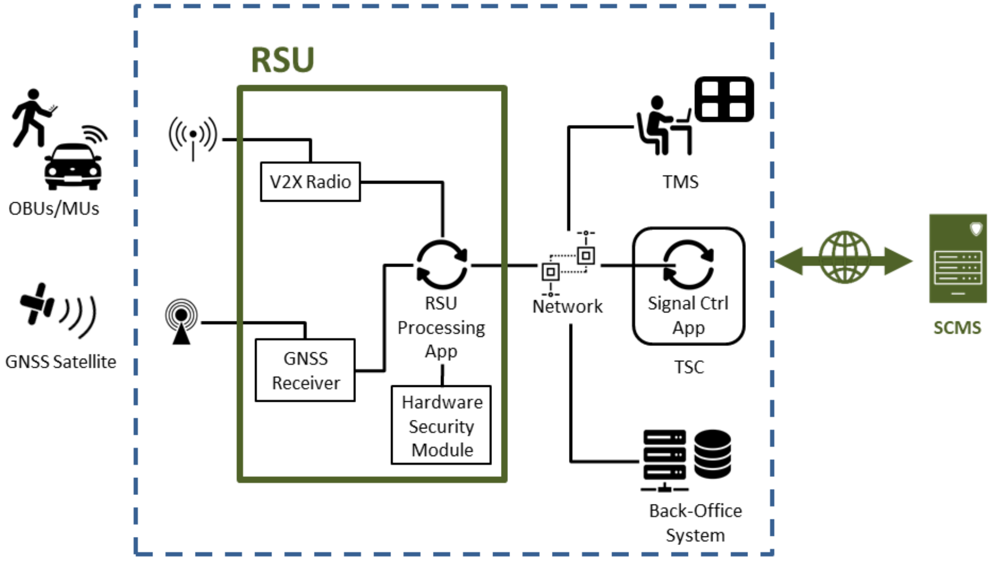


Figure 5. Logical architecture showing an RSU with antennas mounted separately from the unit

2.5 Needs

The RSU serves as the interface between an OBU/MU and the rest of the transportation infrastructure. The purpose of the RSU is to share information among these elements. At a high-level, the services provided by the RSU include the following:

- The RSU provides communication from the OBU/MU to infrastructure elements about their recent history, current status, and future intent.
- The RSU provides communication from infrastructure elements to the OBU/MU about management strategies, signal/device status, incidents, and security services.
- The RSU supports applications that can be used to assist the driver and vehicle systems to improve safety, reduce congestion, and improve travel time predictability.
- The RSU can pre-process data and provide edge computing services for efficient use of the back-office communications and use by other devices such as TSCs.

These high-level services are intended to satisfy the set of needs that are outlined in this document.

The needs identified in the subsections below are written from the perspective of deployers of RSUs and the OBUs and MUs that communicate with them. These needs are summarized as follows:

- General, hardware, and mounting needs that concern the overall RSU device;
- Functional needs that concern the primary operational functions of an RSU;
- Behavioral needs that concern the configuration, management, and monitoring of an RSU;
- Local and back-office interface needs that concern the interoperability with OBUs/MUs, transportation field devices, and back-office systems;
- Security needs that concern V2X interface security, local, and back-office interface security, data integrity, certificate management security, and physical security; and
- Certification of validation needs in verifying critical attributes, essential operations and interoperability for V2X Over-The-Air communication and network data interfacing.

2.5.1 General/Hardware/Mounting

This section identifies needs that concern the overall RSU device.

2.5.1.1 Operating Voltage

The RSU needs to have a nominal operating voltage range conforming to IEEE Std 802.3™-2018 standards. Such voltages allow the use of PoE which facilitates quick installation of RSUs in the field, flexibility in mounting locations, and safety in that PoE voltage and current levels are below those considered dangerous to humans.

2.5.1.2 Extreme Environmental Conditions

The RSU needs to operate under extreme hot, cold, and humid environmental conditions. RSUs operate year-round in the diverse climates of North America including the extremes of Alaska, central Arizona, and the areas surrounding the Gulf of Mexico. They withstand strong winds, rain, flooding, snow and ice and are not susceptible to temperature, water penetration and corrosion.

2.5.1.3 Power Protection and Filtering

The RSU needs to be protected from power surges, power spikes, and electrical noise. RSUs are protected from power and electrical anomalies due to nearby lightning (not direct strikes), utility issues, and malfunctions in adjoining systems. It is recognized that the use of certain technologies may intrinsically help satisfy this need.

2.5.1.4 Withstand Vibration and Shock

The RSU needs to be resistant to vibration and shock. This includes the vibration and shock caused by vehicle traffic, severe weather conditions, and the occasional events such as common carrier shipping, earthquakes, roadwork, and technician handling.

2.5.1.5 Resistant to Electronic Emissions

The RSU needs to be resistant to electromagnetic interference (EMI). Both man-made and natural sources can generate electrical currents and voltages that can inhibit or degrade the performance of electronic devices.

2.5.1.6 Resistant to Out-of-Band and Out-of-Channel Interference

The RSU needs to be resistant to out-of-band and out-of-channel interference. This protects the V2X signal in the operating channel.

2.5.1.7 Resistant to Electrostatic Discharge

The RSU needs to be resistant to electrostatic discharge (ESD). It is common for there to be ESD when maintenance personnel interact with the RSU. RSUs are designed to dissipate ESD to avoid damaging electronic elements.

2.5.1.8 Limit Electronic Emissions

The RSU needs to have limited electronic emissions that cause radio frequency interference (RFI) and electromagnetic interference (EMI). RFI and EMI are limited to not interfere with radios, cell phones, and other electronics in the vicinity of the RSU.

2.5.1.9 Mounting

The RSU needs configurations that facilitate shelf mounting, wall mounting, rack mounting or pole mounting. The RSU may be located within a field cabinet, where it could be shelf, wall or rack mounted. The RSU may also be mounted on a vertical pole or on a horizontal mast arm. Some RSU configurations may involve antennas and radios that are operating remotely from the RSU processor (the RSU can be modular and meets its functionality).

2.5.1.10 Diagnostic Testing

The RSU needs to be designed to support diagnostic testing. This includes the RSU as a whole in addition to individual elements. Maintenance personnel have limited time to confirm proper RSU operation and to identify failed elements. The RSU supports a diagnostic setting in which all messages can be forwarded without verifying signature. The diagnostic setting also supports the storing of messages sent and received.

2.5.1.11 Minimize Time for Maintenance Personnel

The RSU needs to be designed to reduce the time required for maintenance personnel to perform maintenance actions in the field. When an RSU is being repaired there can be a safety hazard for both the motorist and the field maintenance personnel. The RSU is to be designed for quick diagnostics, software updates, antenna replacement/cable, full unit replacement and captive hardware if above the intersection.

2.5.1.12 Quality Construction

The RSU needs to be constructed using quality and safety standards for workmanship, electronic design, and manufacturing. Adherence to applicable standards such as those from the IPC-Association Connecting Electronics Industries and other industry standards is important to developing an RSU that will reliably provide the continuous operation of the system.

2.5.1.13 Interchangeable

The RSU needs to be replaceable by an RSU conformant to this standard. This allows an RSU to be replaced without a change to the hardware interfaces such as connectors and power. This does not limit configurations and features of RSUs which may not be identical.

2.5.1.14 Software and Firmware Updates

The RSU needs to be able to receive and install available software and firmware updates locally and remotely. This facilitates software and firmware updates which increases reliability of the RSU, reduces costs for updates by not requiring bucket trucks, and minimizes effects to traffic flow by avoiding lane closures. Software updates are within the means of the resources on the unit.

2.5.1.15 Size and Weight

The RSU needs to be compact in size and weight based on its installation (Cabinet Mount, Mast Mount, Pole Mount, etc.). RSUs may be installed on signal poles and mast arms where the effects of wind and the weight could hinder deployment.

2.5.1.16 User Safety

The RSU needs to conform to safety requirements for use by field personnel. This includes electrical safety where personnel are protected from high voltage wiring, arc flash hazards, and physical safety from sharp edges.

2.5.2 Functional

This section identifies needs that concern the primary operational functions of an RSU.

2.5.2.1 Startup

The RSU needs to start up using a specific configuration. This includes network and V2X interfaces. This feature allows the operator to configure the state and setup of the RSU when the RSU is powered up.

2.5.2.2 Recovery

The RSU needs to have a remote restart capability with the following configuration options: Factory settings, Default and Last Saved. This includes network and V2X interfaces. This allows the RSU to resume operation or be reconfigured after a power outage or other anomaly. It is desirable that the RSU does not require physical access to recover unless there is a hardware failure.

Note: To restart the RSU locally, the maintenance personnel are expected to recycle the power at the PoE power source.

2.5.2.3 Time Keeping

This section identifies needs regarding time keeping on an RSU.

2.5.2.3.1 Time Accuracy

The RSU needs to accurately maintain time. This feature is critical for RSU management, communications (protocol) and security.

2.5.2.3.2 Time Source

The RSU needs to synchronize to a common time reference used by OBUs/MUs and the surrounding transportation infrastructure. This allows RSU messages (e.g., SPaT) and actions to be conducted based on the same understanding of time.

2.5.2.4 Determine Current Location

The RSU needs to estimate its current location. This feature allows the RSU and its management system to determine the RSU’s location. This facilitates applications that rely on location specific information and monitoring of the RSU’s movement, and to properly correlate its position within the roadway geometry. Cryptographic security processes also use location information.

2.5.2.5 Network Interface

The RSU needs to include a network interface. This is used to connect to the RSCE, TMS and back-office systems and is configured using objects defined in NTCIP 1218 v01.

2.5.2.6 Performance and Monitoring Data

This section identifies needs regarding monitoring data on an RSU.

2.5.2.6.1 Non-Volatile Operational Logging

The RSU needs to include non-volatile log files that record salient events. This is useful for trouble shooting and maintenance.

2.5.2.6.2 Statistical Data

The RSU needs to collect certain statistical data about V2X messages sent and received and V2X devices within range of the RSU. This feature allows the operator to collect trend information and detect significant deviations. This is necessary to help inform the operator of potential issues with radio coverage or changes in V2X device population. An RSU may also be used to assess or confirm the health of other nearby RSUs. The RSU collects GNSS data for analysis to determine the need for providing position correction to OBUs/MUs at that location.

2.5.2.7 RSU Clustering

This section identifies needs regarding coordinating multiple RSUs within same communication zone to improve performance.

2.5.2.7.1 RSU RF Bandwidth

The RSU needs to be able to increase the bandwidth available for use by applications.

2.5.2.8 Message Handling

This section identifies needs regarding the sending and receiving of messages by the RSU. In this case “messages” refers to application data that is exchanged using the WAVE Short Message Protocol (WSMP) as defined in IEEE Std 1609.3™-2020. Refer to NTCIP 1218 v01 for information on how these messages and corresponding behaviors are managed.

Note: This section describes features necessary for secure message handling over the V2X interface. In order to support end-to-end-security, the interface between the back-office/field devices and the RSU is also secure.

2.5.2.8.1 Messages Sent by the RSU

This section identifies needs regarding messages sent by an RSU. It is assumed the messages are already properly encoded.

2.5.2.8.1.1 Immediate Forwarding of Messages Not Signed by the Message Source

The RSU needs to forward messages received from local field devices, back-office systems or TMS to the V2X interface. In this case, the message received is not signed or encrypted, and the RSU signs and may encrypt the message before transmitting it on the V2X interface. This allows the RSU to sign and provide the information to OBUs/MUs that is generated by external devices. For example, a TSC may generate unsigned SPaT and Signal Status (SSM) messages that use this interface. Other examples include information that is displayed on dynamic messages signs.

2.5.2.8.1.2 Immediate Forwarding of Messages Signed by the Message Source

The RSU needs to forward messages received from local field devices, back-office systems or TMS to the V2X interface. In this case the message received is already signed and optionally encrypted, and the RSU forwards it to the V2X interface without additional security processing. This allows the RSU to provide information to OBUs/MUs that is generated by external devices. For example, a TMS or MAP Server may generate signed MAP messages that use this interface.

2.5.2.8.1.3 Storing and Repeating of Messages Not Signed by the Message Source

The RSU needs to periodically transmit messages stored on the RSU. In this case, the stored message is not signed or encrypted, and the RSU signs and may encrypt the message before periodically transmitting it on the V2X interface. This allows the RSU to sign and periodically send a message to OBUs/MUs on behalf of the message source. This interface can be used to support TIM, MAP and other relatively static messages.

2.5.2.8.1.4 Storing and Repeating of Messages Signed by the Message Source

The RSU needs to forward messages received from local field devices, back-office systems or TMS to the V2X interface. In this case the stored message is already signed and may be encrypted, and the RSU periodically transmits it on the V2X interface. This allows the RSU to periodically send a pre-signed message to OBUs/MUs on behalf of the message source. This interface can be used to support TIM, MAP and other relatively static messages that have already been signed.

2.5.2.8.2 Forwarding of Messages Received by the RSU

The RSU needs to forward messages received on the V2X interface to local field devices, back-office systems or TMS, depending on the application content. The received WAVE Short Messages are verified that they are validly signed according to the respective security profile (and decrypted if encryption is used) before forwarding. The RSU will only verify the message if it is being forwarded. This allows the RSU to relay information received from OBUs/MUs to the RSCE (e.g., sending a signal request message to a TSC), TMS, and back-office systems. Note: Diagnostic mode supports forwarding messages without verifying signature.

2.5.2.9 Applications

This section identifies needs regarding the applications that are contained in an RSU.

2.5.2.9.1 SPaT Processing

For a signalized intersection, the RSU needs to broadcast Signal Phase and Timing (SPaT) information in real time. This includes communicating with the TSC to receive SPaT information and converting it to SAE J2735_202007 format. It is intended that the RSU support both the NTCIP 1202 v03A SPaT message and the Traffic Signal Controller Broadcast Message (TSCBM) sent from the TSC. This allows the RSU to provide SPaT to the OBUs/MUs. The TSCBM is defined in the V2I Hub ICD.

Note: Alternatively, the TSC can produce the SPaT message and use an immediate forwarding interface (see Sections 2.5.2.8.1.1 and 2.5.2.8.1.2).

2.5.2.9.2 BSM Pre-Processing

The RSU needs to pre-process Basic Safety Messages (BSMs) to provide statistics to the TMS or back-office system. This enables transportation applications to use BSM information without the RSU forwarding every BSM.

2.5.2.9.3 MAP

The RSU needs to store MAP messages for periodic broadcast over the V2X interface. This allows the OBU/MU to determine which lane it is in and use SPaT information.

Note: Alternatively, the TSC can send the MAP message and use an immediate forwarding interface (see Sections 2.5.2.8.1.1 and 2.5.2.8.1.2).

2.5.2.9.4 Traveler Information

The RSU needs to store TIMs for periodic broadcast over the V2X interface. This feature applies to the SAE J2735_202007 Traveler Information Message (TIM) as well as SAE J2945/3_202003 Road Weather Message (RWM) and the SAE J2945/4 Road Safety Applications currently in development by SAE. This enables the RSU to provide traveler information to OBUs/MUs.

Note: TIMs can be generated by external systems and broadcasted via immediate forwarding. See SAE J2945_201712 for other applications that may generate messages for broadcast via immediate forwarding.

2.5.3 Behavioral

This section identifies needs that concern the configuration, management, and monitoring of an RSU.

2.5.3.1 Configuration and Management

The RSU needs to conform to NTCIP 1218 v01. This enables the IOO to configure and manage the RSU. It is desirable that the RSU does not permit configurations that result in an inoperable state (consistency/integrity checks).

2.5.3.2 Health and Status Monitoring

The RSU needs to perform the monitoring functions described by NTCIP 1218 v01. This enables the IOO to monitor the RSU.

2.5.3.3 Visual Indications

The RSU needs to provide a visual indication of the status of the RSU that is discernable from the ground when mounted. This includes a visual indication of the operating status and the power status of the RSU. This enables field personnel to determine status of the RSU.

2.5.4 Back-Office and V2X Interfaces

This section identifies needs that concern the interoperability with OBUs/MUs and back-office systems.

2.5.4.1 Back-Office Interface

The RSU needs to provide an IP-based communication interface with a traffic management system and/or back-office system. This feature allows operators to monitor RSU operation, to configure all parameters and for data exchange between the systems and the RSU using existing agency IT infrastructure. Access to this interface should be limited to only authorized systems and personnel.

2.5.4.2 V2X Interfaces

This section identifies needs regarding V2X interfaces.

2.5.4.2.1 Radio Interfaces

This section identifies needs for radio interfaces on an RSU. Note that multiple technologies may be supported simultaneously. Other technologies may be developed in the future. This allows the RSU to exchange data with OBUs/MUs and facilitates V2X interoperability.

2.5.4.2.1.1 DSRC (IEEE Std 802.11)

The RSU needs to implement IEEE Std 802.11 (operating outside the context of a BSS (Basic Service Set)). Note: this was originally defined in the 802.11p amendment. This includes supporting operations on multiple channels simultaneously. This allows the RSU to exchange data with OBUs/MUs on multiple channels.

2.5.4.2.1.2 C-V2X (3GPP PC5 Mode 4 (Release 14 or 15))

The RSU needs to implement 3GPP PC5 mode 4.

2.5.4.2.2 Network and Transport Layers

The RSU needs to support the networking and transport protocols defined in IEEE Std 1609™. IEEE Std 1609.3™-2020 defines the networking protocols used by OBUs/MUs to interface with the RSU. This allows the RSU to exchange data with OBUs/MUs.

2.5.5 Security

This section identifies needs that concern V2X interface security, local and back-office interface security, data integrity, certificate management security, and physical security.

2.5.5.1 Authentication

This section identifies needs to authenticate the data exchanged with the RSU.

2.5.5.1.1 Authentication - Messages Sent by the RSU

The RSU needs to apply authentication services to outgoing messages to the OBU/MU. This feature indicates to the OBU/MU that the data transmitted from the RSU is from a "trusted" source.

2.5.5.1.2 Authentication - Messages Received by the RSU

The RSU needs to apply authentication checks to incoming messages form the OBU/MU. This feature also indicates to the IOO that the data received from the OBU/MU is from a "trusted" source and can be used confidently to manage the roadways.

2.5.5.1.3 Authentication - Sender

The RSU needs to be able to apply authentication services on messages in both directions that authenticate that the sender has permissions to send the message being sent.

2.5.5.2 Local and Back Office Interface Security

The RSU needs a secure interface for connection to local field devices and the back office. This interface needs to be secure in the sense that it provides confidentiality, integrity, and authenticity. Authenticity in this sense includes assurance that at the time the RSU first connects to other devices (or, more generally, other parties or entities) on the IOO network, it can be demonstrated to have connected to the intended entity.

2.5.5.3 Data Integrity

The RSU needs to protect data integrity, at rest and in transit, and detect and notify the TMS (RSU management) of integrity losses. This verifies or assists to ensure that the data an RSU transmits is the same as the data the RSU receives from a local field device or back-office system and that it is not corrupted or used in a way it was not intended to.

2.5.5.4 Availability

The RSU needs its data to be available to authorized users and processes in accordance with NTCIP 1218 v01. This verifies or assists to ensure that users and processes are allowed timely and reliable access only to those RSU resources/processes/applications for which they have permissions.

2.5.5.5 Data Confidentiality

The RSU needs to protect the management data exchanged with external devices from unauthorized access. The RSU has to apply confidentiality services to those incoming and outgoing management-related messages that are designated as requiring those services. This protects data that is sensitive (for commercial or other reasons) from being revealed to unauthorized parties.

2.5.5.6 Tamper Evident

The RSU needs to provide tamper-evident mechanisms to identify whether the enclosure has been physically tampered with. This feature allows inspection of RSUs by maintenance personnel to tell whether someone was trying to access or compromise the RSU hardware.

Note: From a security perspective, the enclosure can be that of a traffic signal controller or other device, in which case the tamper evidence requirement shall be fulfilled on that enclosure.

2.5.5.7 Physical Requirement for Private Key Storage

The RSU needs to provide physical protection for access to sensitive information (e.g., private keys) stored on its security module. Having adequate security protections for cryptographic material is a prerequisite for enrollment of the RSU in the Security Credential Management System (SCMS). Tamper-evident mechanisms on the security module should include methods or utilities for resetting the tamper status for maintenance personnel in the event of self-servicing.

Notes:

a) It is important to differentiate that this need aims to protect cryptographic information stored inside the RSU's hardware security module (HSM) from a malicious actor gaining access. The same level of security may not be needed for protecting physical access to the RSU hardware in general.
b) Cryptographic keys used for signing V2X messages need a higher level of protection, including automatically be destroyed when tampering with the HSM itself is detected.
c) Information which is usually broadcast via the V2X interface in readable form (e.g., MAP or TIM messages) is not considered confidential information. Those messages are signed (secure) to protect data integrity and to verify or assist in ensuring the origin is a trusted source.

2.5.5.8 System Defaults

The RSU needs to disable or reset any services, applications, and communications parameters that are not utilized by default. This feature causes the RSU to address potential security vulnerabilities that may exist because of default settings.

2.5.5.9 Connection Assurance

The RSU needs to have assurance of connectivity to and access by the correct network.

2.5.5.10 Secure Credential Management System

This section identifies needs concerning the management of the RSU interface to an SCMS.

Note that there may be different security certificates for each application supported by the RSU.

2.5.5.10.1 SCMS Enrollment

The RSU needs the capability to enroll with an SCMS provider. RSUs enroll (and re-enroll) with an SCMS provider to request application certificates that they can use to sign messages. Note: Enrollment processes, including requirements on the environment in which enrollment is to take place, are defined by the SCMS provider.

2.5.5.10.2 RSU Configurability for SCMS

The RSU needs to have the ability to be configured for SCMS interaction. This feature allows the IOO to configure what applications the RSU requests certificates for and when the RSU will request new certificates.

2.5.5.10.3 SCMS Connectivity

The RSU needs to connect to an SCMS to request and download new application certificates. This feature allows the RSU to sign messages.

2.5.5.10.4 Store Certificates and Associated Private Keys

The RSU needs to securely store the enrollment certificates, application certificates and trust chain files from unauthorized modification and substitution. The RSU needs to store the private keys associated with enrollment and application certificates in a way that protects them from unauthorized use.

2.5.5.10.5 Download CRLs

The RSU needs to download all the relevant Certificate Revocation Lists (CRL) from the SCMS so the RSU can authenticate signed messages from other devices.

2.5.5.10.6 Download SCMS Files

The RSU needs to download other files associated with the SCMS and certificate operations such as local certificate chain file (LCCF). The LCCF is used by devices to determine what certificate authorities (CAs) are in the chain of trust. This feature allows devices to rapidly verify incoming signed messages even though the CA certificate is not included in those messages.

2.5.5.11 Secure Administration

The RSU needs to provide a secure interface for an administrator to remotely configure the RSU. This allows an administrator to access the RSU and perform administration functions, such as configuring security features.

2.5.5.12 Secure Management of Credentials

The RSU needs to have secure management of all credentials.

2.5.5.13 Logging for General and Security Purposes

The RSU needs to support logging operations for security purposes.

2.5.5.14 Secure Updates

The RSU needs to support updates to software/firmware in a secure fashion.

2.5.5.15 Support SCMS for OBUs/MUs

The RSU provides the ability for an OBU/MU to connect to an SCMS

2.6 Operational Policies and Constraints

The RSU is expected to comply with applicable Federal and State regulations. The applicable regulations may vary by jurisdiction but includes portions of radio regulations such as CFR Title 47 - Telecommunication: Parts 15, 90 and 95; and the National Electrical Code.

2.7 Relationship to ARC-IT [Informative]

This section describes which portions of the Architecture Reference for Cooperative and Intelligent Transportation, known as ARC-IT are addressed by the standard. Figure 6 shows the key interfaces from ARC-IT for an RSU (referred to as Connected Vehicle Roadside Equipment in ARC-IT). The diagram shows the key elements of this standard mapped to the classes of Physical Objects from the Physical View of ARC-IT: Field, Center, Vehicle, and Personal. In ARC-IT, a Physical Object is a system or device that provides ITS functionality as part of ITS.

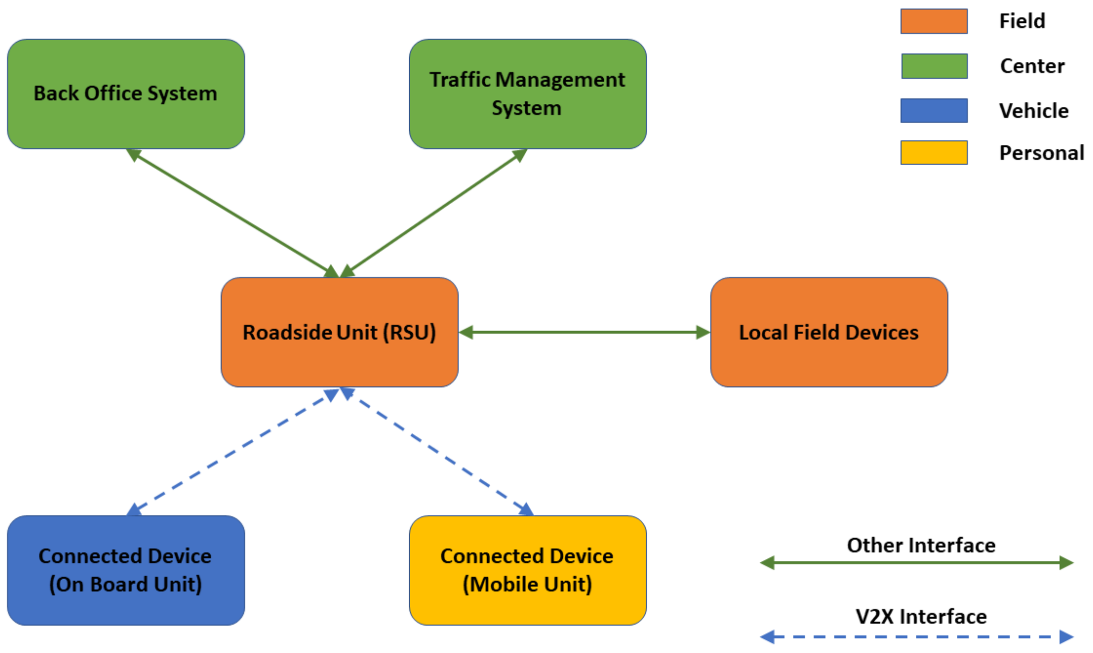


Figure 6. ARC-IT Physical View

ARC-IT identifies a set of over 200 information flows that interface between the RSU, represented in ARC-IT as Connected Vehicle Roadside Equipment (CVRE), and the elements in Figure 6. An information flow represents information that is exchanged between the physical objects, and many of those information flows are addressed in this standard.

The Physical View of ARC-IT also defines the functions, called Functional Objects (FO), of a Physical Object. ARC-IT describes over 30 FOs that define the potential functionality of an RSU, and some of the FOs covered by this standard are listed below. As ARC-IT is constantly updated, not all the FOs are listed here, but the complete list and descriptions of FOs can be found on the ARC-IT website.

- **RSE Data Subscription Management.** This FO manages data subscriptions for an RSE. It provides access to a catalog of available data, manages the necessary identification information and rules that govern the data subscriptions, supports communications with data providers to collect data per the subscription rules, and makes the data available to other RSE applications. It supports different mechanisms for collecting data including one-time query-response as well as publish-subscribe services.

- **RSE Device Management.** This FO provides executive control and monitoring of the RSE hardware and installed software applications. It monitors the operational status of the hardware and other attached field devices and detects and reports fault conditions. A back-office interface supports application installation, upgrade, and configuration as well as remote control of the operating mode and hardware configuration settings and initiation of remote diagnostics. A local interface is provided to field personnel for local monitoring and diagnostics, supporting field maintenance, repair, and replacement.
- **RSE Intersection Management.** This FO uses short range communications to support connected vehicle applications that manage signalized intersections. It communicates with approaching vehicles and ITS infrastructure (e.g., the TSC) to enhance traffic signal operations. Coordination with the ITS infrastructure also supports conflict monitoring to ensure the RSE output and traffic signal control output are consistent and degrade in a fail-safe manner.
- **RSE Support Services.** This FO provides foundational functions that support data collection, management, location reference, timing, and data distribution. It coordinates with Support subsystems to maintain necessary registrations with respect to location and scope. It maintains precise location and time information to support other services.

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) Needs to Requirements Traceability Matrix (NRTM) – 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 NRTM. The NRTM also indicates which of the items are mandatory, conditional, or optional. The NRTM 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) Requirements – These are requirements that collectively satisfy the user needs identified in Section 2.5. These requirements provide the details so that a requirement can be fulfilled and validated.

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 of this RSU standard. For these readers, Section 3.2.3 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 for this standard. Table 9 in Section 3.2.3 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 NRTM that traces each user need to one or more requirements defined in this section. The details of each requirement are then presented following the NRTM.

3.2 Needs to Requirements Traceability Matrix

The NRTM, provided in Table 9 defined in Section 3.2.3, maps the user needs defined in Section 2 to the requirements defined in Section 3. The NRTM 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 device manufacturer and user, as a detailed indication of the capabilities of the implementation.
c) A user, as a basis for initially checking the potential interoperability with another implementation.
d) A tester, as a checklist to compare against a specification and provide basis for test planning.

3.2.1 Notation [Informative]

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

3.2.1.1 Conformance Symbols

The symbols in Table 5 are used to indicate status under the Conformance column in the NRTM.

Table 5. 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."

3.2.1.2 Conditional Status Notation

The predicate notations in Table 6 may be used.

Table 6. 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 NRTM states that the feature or features identified by the predicate are supported. In the simplest case, <predicate> is the identifying tag of a single NRTM 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. The symbol <predicate> also may be a Boolean expression composed of several indices. "AND", "OR", and "NOT" shall be used to indicate the Boolean logical operations.

The predicates used in this standard map to the sections indicated in Table 7.

Table 7. Predicate Mapping

Predicate	Section
1609.2.1	3.3.5.10.1.3
802.11	3.3.4.2.1.2.1
CAMP	3.3.5.10.1.2
PC5	3.3.4.2.1.3.1
Pole	3.3.1.9.1

3.2.1.3 Support Column Symbols

The Support column in the NRTM 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 8. Support Column Entries

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

3.2.2 Instructions for Completing the NRTM [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.

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

3.2.2.1 Conformance Definition

To claim "Conformance" to this standard, the manufacturer shall minimally fulfill the mandatory requirements as identified in the NRTM (see Table 9).

Note: The reader and user of this standard is advised that 'conformance' to RSU Standard v01 should not be confused with 'compliance' to a specification. RSU Standard v01 is as broad as possible to allow a very simple RSU implementation to be 'conformant' to RSU Standard 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 RSU Standard v01 to achieve interoperability. This means that functions and requirements defined as 'optional' in RSU Standard 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 RSU Standard v01 and the standards it references (e.g., IEEE Std 1609). 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 NRTM, 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.

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.

3.2.2.2 NTCIP 1218 v01 PRL

A large number of requirements in this RSU Standard point to specific requirements defined in NTCIP 1218 v01, Object Definitions for Roadside Units. NTCIP 1218 v01 is therefore a companion standard to this RSU Standard, and as such the Protocol Requirements List (PRL) should be completed in full in addition to the completing the NRTM for this standard in the next section (Section 3.2.3). The PRL for NTCIP 1218 v01 can be found in Table 6, Section 3.3.3 of NTCIP 1218 v01. Note: the PRL and the NRTM are used exactly the same way, with the same columns, except it is called a PRL in the NTCIP family of standards.

3.2.3 NRTM

In addition to the Conformance column and the Support column, which were discussed in Sections 3.2.1.1 and 3.2.1.3, the additional columns in the NRTM 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 NRTM is based upon the user needs 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 NRTM references the traces from user needs to these requirements.

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.

Table 9. Needs to Requirements Traceability Matrix (NRTM)

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
2.5	Needs					
2.5.1	General/Hardware/Mounting					
2.5.1.1	Operating Voltage			M	Yes	
		3.3.1.1	Power-over-Ethernet Plus (POE+)	M	Yes	
2.5.1.2	Extreme Environmental Conditions			M	Yes	
		3.3.1.2.1	Ambient Temperature RSU	M	Yes	
		3.3.1.2.2	Ambient Temperature Rate of Change RSU	M	Yes	
		3.3.1.2.3	Storage Temperature RSU	M	Yes	
		3.3.1.2.4	Humidity RSU	M	Yes	
		3.3.1.2.5	Rain Resistance Test	Pole:M	Yes / NA	
		3.3.1.2.6	Corrosion Resistance Enclosure	Pole:M	Yes / NA	
		3.3.1.2.7	Corrosion Resistance Test	Pole:M	Yes / NA	
2.5.1.3	Power Protection and Filtering			M	Yes	
		3.3.1.3.1	Transients	M	Yes	
		3.3.1.3.2	Surges	M	Yes	
2.5.1.4	Withstand Vibration and Shock			M	Yes	
		3.3.1.4.1	Vibration	M	Yes	
		3.3.1.4.2	Shock	M	Yes	
		3.3.1.4.3	Operational Vibration Test	M	Yes	
		3.3.1.4.4	Non-Operational Shock Test	M	Yes	
2.5.1.5	Resistant to Electronic Emissions			M	Yes	
		3.3.1.5	Resistance to Electronic Emissions	M	Yes	
2.5.1.6	Resistant to Out-of-Band and Out-of-Channel Interference			M	Yes	
		3.3.1.6.1	IEEE Std 802.11 Out-of-Band and Out-of-Channel Interference Requirements	802.11:M	Yes / NA	
		3.3.1.6.2	3GPP PC5 Mode 4 (Release 14 or 15) Out-of-Band and Out-of-Channel Interference Requirements	PC5:M	Yes / NA	
2.5.1.7	Resistant to Electrostatic Discharge			M	Yes	
		3.3.1.7	Resistant to Electrostatic Discharge	M	Yes	
2.5.1.8	Limit Electronic Emissions			M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		3.3.1.8.1	Electronic Emissions	M	Yes	
		3.3.1.8.2	IEEE Std 802.11 Emissions Mask	802.11:M	Yes / NA	
		3.3.1.8.3	3GPP PC5 Mode 4 (Release 14 or 15) Emissions Mask	PC5:M	Yes / NA	
2.5.1.9	Mounting			M	Yes	
		3.3.1.9.1 (Pole)	RSU Pole Mounting Requirements	O.1 (1)	Yes / No	Additional requirements to be specified by the procuring agency.
		3.3.1.9.2	RSU Rack Mounting Requirements	O.1 (1)	Yes / No	
		3.3.1.9.3	RSU Shelf Mounting Requirements	O.1 (1)	Yes / No	
		3.3.1.9.4	RSU Wall Mounting Requirements	O.1 (1)	Yes / No	
2.5.1.10	Diagnostic Testing			M	Yes	
		3.3.1.10.1	Diagnostic Setting – Forwarding Received Messages	O	Yes / No	See NTCIP 1218 v01: Requirements 3.5.1.2.2.3.8 and 3.5.1.2.2.3.9
		3.3.1.10.2	Diagnostic Setting - Forwarding Transmitted Messages	O	Yes / No	See NTCIP 1218 v01: Requirements 3.5.1.2.2.4.1, 3.5.1.2.2.4.2, 3.5.1.2.2.4.3, 3.5.1.2.2.4.4, and 3.5.1.2.2.4.5
		3.3.1.10.3	Diagnostic Setting - Storing Sent and Received Messages	O	Yes / No	See NTCIP 1218 v01: Requirements 3.5.1.2.3.1, 3.5.1.2.3.2, and 3.5.1.2.3.5
		3.3.1.10.4	Diagnostic Setting – Features Accessible through SNMP	M	Yes	
		3.3.1.10.5	Diagnostic Setting – Transmitting without Signature	O	Yes / No	
2.5.1.11	Minimize Time for Maintenance Personnel			M	Yes	
		3.3.1.11.1.1	Power Indication	M	Yes	
		3.3.1.11.1.2	Power Indication Location	M	Yes	
		3.3.1.11.1.3	Power LED Characteristics	M	Yes	
		3.3.1.11.2.1	Status Indication	M	Yes	
		3.3.1.11.2.2	Status Indication Location	M	Yes	
		3.3.1.11.2.3	Status LED Characteristics	M	Yes	
2.5.1.12	Quality Construction			M	Yes	
		3.3.1.12.1	Edges	M	Yes	
		3.3.1.12.2	Non-Electronic Hardware Materials	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		3.3.1.12.3	Electrical Isolation and Equipment Grounding	O, Pole:M	Yes / No / NA	
		3.3.1.12.4	Electrical Installation and Integration	M	Yes	
		3.3.1.12.5.1	Maximum Ratings	M	Yes	
		3.3.1.12.5.2	PCB Locking Devices	M	Yes	
		3.3.1.12.6	Manufacturer's Specifications	M	Yes	
		3.3.1.12.7	Enclosure Surface Ultraviolet Protection (Discoloring)	Pole:M	Yes / NA	
2.5.1.13	Interchangeable			M	Yes	
		3.3.1.13.1	Ethernet Connector	M	Yes	
		3.3.1.13.2	Powered Connector	M	Yes	
		3.3.1.13.3	Antenna Connectors	O	Yes / No	
		3.3.1.13.4	Open Standards	M	Yes	
		3.3.1.13.5	Management Information Base	M	Yes	
		3.3.1.13.6	Communications Interface	M	Yes	
2.5.1.14	Software and Firmware Updates			M	Yes	
		3.3.1.14	Software and Firmware Updates Requirements	M	Yes	See NTCIP 1218 v01: Requirements 3.5.1.1.5.1, 3.5.1.1.5.2, and 3.5.1.1.5.3.
2.5.1.15	Size and Weight			Pole:M	Yes / NA	
		3.3.1.15.1	Weight	M	Yes	
		3.3.1.15.2	Size	M	Yes	
2.5.1.16	User Safety			M	Yes	
		3.3.1.16	User Safety Requirements	M	Yes	
2.5.2	Functional					
2.5.2.1	Startup			M	Yes	
		3.3.2.1.1	RSU Startup Functions	M	Yes	See NTCIP 1218 v01: Requirements 3.5.1.1.4.2, 3.5.1.1.4.3, 3.5.1.1.4.4 and 3.5.1.1.4.5.
		3.3.2.1.2	RSU Restarts	M	Yes	See NEMA TS 10-2020.
		3.3.2.1.3	RSU Transition from Startup	M	Yes	
		3.3.2.1.4	Application Configuration	M	Yes	See NTCIP 1218 v01: Requirements 3.5.1.4.2.1 and 3.5.1.4.2.2.
2.5.2.2	Recovery			M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		3.3.2.2.1	Remote Restart	M	Yes	See NTCIP 1218 v01: Requirement 3.5.3.3.
		3.3.2.2.2	Factory Settings	O	Yes / No	
		3.3.2.2.3	Default Settings	O	Yes / No	
		3.3.2.2.4	Log Restarts	M	Yes	
2.5.2.3	Time Keeping					
2.5.2.3.1	Time Accuracy			M	Yes	
		3.3.2.3.1.1	Time Reference	M	Yes	
		3.3.2.3.1.2	Time Output	M	Yes	
		3.3.2.3.1.3	Time Accuracy - Primary Time Source	M	Yes	
		3.3.2.3.1.4	Leap Seconds	M	Yes	
2.5.2.3.2	Time Source			M	Yes	
		3.3.2.3.2.1	Primary Time Source	M	Yes	
		3.3.2.3.2.2	Report Primary Time Source	M	Yes	See NTCIP 1218 v01: Requirements 3.5.2.3.1
		3.3.2.3.2.3	Secondary Time Source	M	Yes	
		3.3.2.3.2.4	Maintain Operations	M	Yes	
		3.3.2.3.2.5	Log Time Failures	M	Yes	
		3.3.2.3.2.6	Time Source Server	O	Yes / No	
2.5.2.4	Determine Current Location			M	Yes	
		3.3.2.4.1	Location Source	M	Yes	See NTCIP 1218 v01: Requirements 3.5.2.4.2
		3.3.2.4.2	Report Location	M	Yes	See NTCIP 1218 v01: Requirements 3.5.2.4.1, 3.5.2.4.5
		3.3.2.4.3	Location Status	M	Yes	See NTCIP 1218 v01: Requirements 3.5.2.4.2
		3.3.2.4.4	Log Location Failure – Satellites	M	Yes	
2.5.2.5	Network Interface			M	Yes	
		3.3.2.5	Network Interface Requirement	M	Yes	See NTCIP 1218 v01: Requirements 3.5.1.2.1.2
2.5.2.6	Performance and Monitoring Data					
2.5.2.6.1	Non-Volatile Operational Logging			M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		3.3.2.6.1	Operational Logging	M	Yes	See NTCIP 1218 v01: Requirements 3.4.2.3, 3.6.3.1, 3.6.3.2, 3.6.3.3, 3.6.3.4, 3.6.3.5, 3.6.3.6, and 3.6.3.7
2.5.2.6.2	Statistical Data			M	Yes	
		3.3.2.6.2.1	Log Interface Data	O.2 (1..*)	Yes / No	See NTCIP 1218 v01: Requirements 3.5.1.2.3.2, 3.5.1.2.3.3, 3.5.1.2.3.4, 3.5.1.2.3.5, 3.5.1.2.3.6, 3.5.1.2.3.7, 3.5.1.2.3.8, 3.5.1.2.3.9, 3.5.1.2.3.10, and 3.5.1.2.3.11
		3.3.2.6.2.2	Log RF Communications Reception Coverage	O.2 (1..*)	Yes / No	See NTCIP 1218 v01: Requirements 3.5.2.8.2, 3.5.2.8.3, 3.5.2.8.4, 3.5.2.8.5, 3.5.2.8.6, and 3.5.2.8.7
		3.3.2.6.2.3	Report Number of Messages Exchanged by the V2X Radio	O.2 (1..*)	Yes / No	See NTCIP 1218 v01: Requirements 3.5.2.6
2.5.2.7	RSU Clustering					
2.5.2.7.1	RSU RF Bandwidth			O	Yes / No	
		3.3.2.7.1.1	Configure Radio as a Service RSU	802.11:M	Yes / NA	
2.5.2.8	Message Handling					
2.5.2.8.1	Messages Sent by the RSU					
2.5.2.8.1.1	Immediate Forwarding of Messages Not Signed by the Message Source			M	Yes	
		3.3.2.8.1.1	Signing and Forwarding of Messages Not Signed by the Message Source	M	Yes	See NTCIP 1218 v01: Requirements 3.5.1.2.2.2.1, 3.5.1.2.2.2.2, 3.5.1.2.2.2.3, 3.5.1.2.2.2.4, 3.5.1.2.2.2.5, 3.5.1.2.2.2.6, and 3.5.1.2.2.2.7
		3.3.2.8.3.1	Time Critical Messages	M	Yes	
		3.3.2.8.3.2	Non-Time Critical Messages	M	Yes	
2.5.2.8.1.2	Immediate Forwarding of Messages Signed by the Message Source			M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	User Need	FR ID	Functional Requirement	Conformance	Support	Additional Specifications
		3.3.2.8.1.2	Forwarding of Messages Signed by the Message Source	M	Yes	See NTCIP 1218 v01: Requirements 3.5.1.2.2.2.1, 3.5.1.2.2.2.2, 3.5.1.2.2.2.3, 3.5.1.2.2.2.4, 3.5.1.2.2.2.5, 3.5.1.2.2.2.6, and 3.5.1.2.2.2.7
		3.3.2.8.3.1	Time Critical Messages	M	Yes	
		3.3.2.8.3.2	Non-Time Critical Messages	M	Yes	
2.5.2.8.1.3	Storing and Repeating of Messages Not Signed by the Message Source			M	Yes	
		3.3.2.8.1.3	Storing and Repeating Messages Not Signed by the Message Source	M	Yes	See NTCIP 1218 v01: Requirements 3.5.1.2.2.1.1, 3.5.1.2.2.1.2, 3.5.1.2.2.1.3, 3.5.1.2.2.1.4, 3.5.1.2.2.1.5, 3.5.1.2.2.1.6, 3.5.1.2.2.1.7, 3.5.1.2.2.1.8, 3.5.1.2.2.1.9, 3.5.1.2.2.1.10, 3.5.1.2.2.1.11, 3.5.1.2.2.1.12, and 3.5.1.2.2.1.13
2.5.2.8.1.4	Storing and Repeating of Messages Signed by the Message Source			M	Yes	
		3.3.2.8.1.4	Storing and Repeating Messages Signed by the Message Source	M	Yes	See NTCIP 1218 v01: Requirements 3.5.1.2.2.1.1, 3.5.1.2.2.1.2, 3.5.1.2.2.1.3, 3.5.1.2.2.1.4, 3.5.1.2.2.1.5, 3.5.1.2.2.1.6, 3.5.1.2.2.1.7, 3.5.1.2.2.1.8, 3.5.1.2.2.1.9, 3.5.1.2.2.1.10, 3.5.1.2.2.1.11, 3.5.1.2.2.1.12, and 3.5.1.2.2.1.13
2.5.2.8.2	Forwarding of Messages Received by the RSU			M	Yes	
		3.3.2.8.2	Forwarding of Messages Received by the RSU	M	Yes	See NTCIP 1218 v01: Requirements 3.5.1.2.2.3.1, 3.5.1.2.2.3.2, 3.5.1.2.2.3.3, 3.5.1.2.2.3.4, 3.5.1.2.2.3.5, 3.5.1.2.2.3.6, 3.5.1.2.2.3.7, 3.5.1.2.2.3.8, 3.5.1.2.2.3.9, and 3.5.1.2.2.3.10
		3.3.2.8.3.1	Time Critical Messages	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		3.3.2.8.3.2	Non-Time Critical Messages	M	Yes	
2.5.2.9	Applications					
2.5.2.9.1	SPaT Processing			O	Yes / No	
		3.3.2.9.1.1	NTCIP 1202	O.3 (1..*)	Yes / No	
		3.3.2.9.1.2	TSCBM	O.3 (1..*)	Yes / No	
2.5.2.9.2	BSM Pre-Processing			O	Yes / No	
		3.3.2.9.2.1	BSM Filtering	M	Yes	The RSU shall support a minimum of ___ (4-255, Default=4) zones.
		3.3.2.6.2.1	Log Interface Data	O.2 (1..*)	Yes / No	See NTCIP 1218 v01: Requirements 3.5.1.2.3.2, 3.5.1.2.3.3, 3.5.1.2.3.4, 3.5.1.2.3.5, 3.5.1.2.3.6, 3.5.1.2.3.7, 3.5.1.2.3.8, 3.5.1.2.3.9, 3.5.1.2.3.10, and 3.5.1.2.3.11
		3.3.2.6.2.2	Log RF Communications Reception Coverage	O.2 (1..*)	Yes / No	See NTCIP 1218 v01: Requirements 3.5.2.8.2, 3.5.2.8.3, 3.5.2.8.4, 3.5.2.8.5, 3.5.2.8.6, and 3.5.2.8.7
		3.3.2.6.2.3	Report Number of Messages Exchanged by the V2X Radio	O.2 (1..*)	Yes / No	See NTCIP 1218 v01: Requirements 3.5.2.6
2.5.2.9.3	MAP			M	Yes	
		3.3.2.8.1.3	Storing and Repeating Messages Not Signed by the Message Source	O.4 (1..*)	Yes / No	
		3.3.2.8.1.4	Storing and Repeating Messages Signed by the Message Source	O.4 (1..*)	Yes / No	
2.5.2.9.4	Traveler Information			M	Yes	
		3.3.2.8.1.3	Storing and Repeating Messages Not Signed by the Message Source	O.5 (1..*)	Yes / No	
		3.3.2.8.1.4	Storing and Repeating Messages Signed by the Message Source	O.5 (1..*)	Yes / No	
2.5.3	Behavioral			M	Yes	
2.5.3.1	Configuration and Management			M	Yes	
		3.3.3.1.1	Retrieve RSU Identity	M	Yes	See NTCIP 1218 v01: Requirements 3.5.1.1.1.1, 3.5.1.1.1.2, 3.5.1.1.1.3, 3.5.1.1.1.4, and 3.5.1.1.1.5

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	User Need	FR ID	Functional Requirement	Conformance	Support	Additional Specifications
		3.3.3.1.2	Retrieve Configuration Version of the RSU	M	Yes	See NTCIP 1218 v01: Requirement 3.5.1.1.1.2
		3.3.3.1.3	Configure RSU Location	M	Yes	See NTCIP 1218 v01: Requirements 3.5.1.1.3.1, 3.5.1.1.3.2, 3.5.1.1.3.3, and 3.5.1.1.3.4
		3.3.3.1.4	Notifications	M	Yes	See NTCIP 1218 v01: Requirements 3.5.1.1.7.1, 3.5.1.1.7.2, 3.5.1.1.7.3.x, 3.5.1.1.7.4, 3.5.1.1.7.5, and 3.5.1.1.7.6
		3.3.3.1.5	Configuration Error Resilience	M	Yes	
		3.3.3.1.6	Control Mode of Operation	M	Yes	See NTCIP 1218 v01: Requirements 3.5.3.1
		3.3.3.1.7	Control RF Antenna Output	M	Yes	See NTCIP 1218 v01: Requirements 3.5.3.2
		3.3.3.1.8	Control Application	M	Yes	See NTCIP 1218 v01: Requirements 3.5.3.4
2.5.3.2	Health and Status Monitoring			M	Yes	
		3.3.3.2.1	Determine Mode of Operations	M	Yes	See NTCIP 1218 v01: Requirements 3.5.2.2
		3.3.3.2.2	Monitor Current Status	M	Yes	See NTCIP 1218 v01: Requirements 3.5.1.3.3.1.1, 3.5.1.3.3.1.7, 3.5.1.3.1.5, 3.5.2.2, 3.5.2.3.1, 3.5.2.3.2, 3.5.2.11.1, and 3.5.2.11.2.1
		3.3.3.2.3	Determine Operational Performance	M	Yes	See NTCIP 1218 v01: Requirements 3.5.2.1.1, 3.5.2.1.2, 3.5.2.1.3, 3.5.2.1.4, 3.5.2.1.5, 3.5.2.1.6, 3.5.2.1.7, and 3.5.2.1.8
		3.3.3.2.4	Determine Operating Environment	O	Yes / No	See NTCIP 1218 v01: Requirements 3.5.2.10.1, 3.5.2.10.2
2.5.3.3	Visual Indications			M	Yes	
		3.3.1.11.1.1	Power Indication	M	Yes	
		3.3.1.11.1.2	Power Indication Location	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		3.3.1.11.1.3	Power LED Characteristics	M	Yes	
		3.3.1.11.2.1	Status Indication	M	Yes	
		3.3.1.11.2.2	Status Indication Location	M	Yes	
		3.3.1.11.2.3	Status LED Characteristics	M	Yes	
2.5.4	Back-Office and V2X Interfaces					
2.5.4.1	Back-Office Interface			M	Yes	
		3.3.2.5	Network Interface Requirement	M	Yes	
		3.3.4.1	Back-Office Interface Requirement	M	Yes	See NTCIP 1218 v01: Requirements 3.5.1.2.1.1, 3.5.1.2.1.2, and 3.5.1.2.1.3
2.5.4.2	V2X Interfaces					
2.5.4.2.1	Radio Interfaces			M	Yes	Note: Additional Guidance has not been developed for dual active mode.
2.5.4.2.1.1 (802.11)	DSRC (IEEE Std 802.11)			O.6 (1..*)	Yes / No	
		3.3.4.2.1.1.1	Transmit Power Range and Accuracy	M	Yes	
		3.3.4.2.1.1.2	Transmit Power Monotonicity	M	Yes	
		3.3.4.2.1.2.1	DSRC (IEEE Std 802.11)	M	Yes	
		3.3.4.2.1.2.2	Receiver Sensitivity (DSRC)	M	Yes	
		3.3.4.2.1.2.3	Multi-Channel Operations	M	Yes	See NTCIP 1218 v01: Requirements 3.5.1.3.3.3
			Maintain Channel Switching Operations	M	Yes	
2.5.4.2.1.2 (PC5)	C-V2X (3GPP PC5 Mode 4 (Release 14 or 15))			O.6 (1..*)	Yes / No	See SAE J3161 for more guidance on configuring the PC5 interface.
		3.3.4.2.1.1.1	Transmit Power Range and Accuracy	M	Yes	
		3.3.4.2.1.1.2	Transmit Power Monotonicity	M	Yes	
		3.3.4.2.1.3.1	C-V2X (3GPP PC5 Mode 4 (Release 14 or 15)) - Channel 183	M	Yes	
		3.3.4.2.1.3.2	C-V2X (3GPP PC5 Mode 4 (Release 14 or 15)) - Channel 180	O	Yes / No	
		3.3.4.2.1.3.3	Receiver Sensitivity (C-V2X)	M	Yes	
2.5.4.2.2	Network and Transport Layers			M	Yes	
		3.3.4.2.2.1	WAVE	M	Yes	
		3.3.4.2.2.2	WAVE Short Message Protocol	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		3.3.4.2.2.3	Internet Protocol	M	Yes	
		3.3.4.2.2.4	WAVE Service Advertisement	M	Yes	See NTCIP 1218 v01: Requirements 3.5.1.3.3.2
		3.3.4.2.2.5	WAVE Router Advertisement	O	Yes / No	See NTCIP 1218 v01: Requirements 3.5.1.3.3.2.4
2.5.5	Security			M	Yes	
2.5.5.1	Authentication			M	Yes	
2.5.5.1.1	Authentication - Messages Sent by the RSU			M	Yes	
		3.3.5.1.1	V2X Interface Security - Sending Messages	M	Yes	
2.5.5.1.2	Authentication - Messages Received by the RSU			M	Yes	
		3.3.5.1.2	V2X Interface Security - Receiving and Forwarding Messages	M	Yes	
2.5.5.1.3	Authentication - Sender			M	Yes	
		3.3.5.1.1	V2X Interface Security - Sending Messages	M	Yes	
		3.3.5.1.2	V2X Interface Security - Receiving and Forwarding Messages	M	Yes	
2.5.5.2	Local and Back Office Interface Security			M	Yes	
		3.3.5.2	Local and Back-Office Interface Security Requirements	M	Yes	
2.5.5.3	Data Integrity			M	Yes	
		3.3.5.3.1	Data Integrity - At Rest	M	Yes	
		3.3.5.3.2	Data Integrity - In Transit	M	Yes	See NTCIP 1218 v01: Requirement 3.6.1.2.1.
		3.3.5.3.3	Device Integrity - Notification	M	Yes	See NTCIP 1218 v01: Requirements 3.5.1.1.7.3.1 and 3.5.1.1.7.3.2.
2.5.5.4	Availability			M	Yes	
		3.3.5.4.1	Manage Availability Requirements	M	Yes	See NTCIP 1218 v01: Requirements 3.5.4.2.1, and 3.5.4.2.2
		3.3.5.4.2	Device Auditing Requirements	M	Yes	See NTCIP 1218 v01: Requirement 3.5.1.1.7.3.5.
2.5.5.5	Data Confidentiality			M	Yes	

Needs to Requirements Traceability Matrix (NRTM)

User Need ID	User Need	FR ID	Functional Requirement	Conformance	Support	Additional Specifications
		3.3.5.5	Data Confidentiality Requirements	M	Yes	See NTCIP 1218 v01: Requirements 3.6.1.2.1, 3.6.1.2.2, 3.6.1.2.3, and 3.6.1.2.4
2.5.5.6	Tamper Evident			M	Yes	
		3.3.5.6.1	Tamper Evident Enclosure - Visual Requirements	M	Yes	
		3.3.5.6.2	Tamper Evident Unused Port Requirements	O	Yes / No	
		3.3.5.6.3	Tamper Evident Enclosure - Bootup Requirements	O	Yes / No	
2.5.5.7	Physical Requirement for Private Key Storage			M	Yes	
		3.3.5.7	Private Key Storage Requirements	M	Yes	
2.5.5.8	System Defaults			M	Yes	
		3.3.5.8.1	RSU OS Applications and Services	M	Yes	
		3.3.5.8.2	RSU OS Ports and Protocols	M	Yes	
		3.3.5.8.3	RSU Password	M	Yes	
2.5.5.9	Connection Assurance			M	Yes	
		3.3.5.9.1	Assurance of Correct Connection Requirement	M	Yes	
		3.3.5.9.2	Assurance of Continued Correct Connection Requirement	M	Yes	
2.5.5.10	Secure Credential Management System					
2.5.5.10.1	SCMS Enrollment			M	Yes	
		3.3.5.10.1.1	SCMS Enrollment Requirement - Bootstrapping	M	Yes	
		3.3.5.10.1.2 (CAMP)	SCMS Enrollment Requirement - CAMP	O.7 (1..*)	Yes / No / NA	The following is a list of acceptable SCMS providers: ______________________________ ______________________________
		3.3.5.10.1.3 (1609.2.1)	SCMS Enrollment Requirement - IEEE Std 1609.2.1	O.7 (1..*)	Yes / No / NA	The following is a list of acceptable SCMS providers: ______________________________ ______________________________
2.5.5.10.2	RSU Configurability for SCMS			M	Yes	
		3.3.5.10.2	SCMS Configurability Requirement	M	Yes	
2.5.5.10.3	SCMS Connectivity			M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		3.3.5.10.3.1	SCMS Connectivity Requirement - CAMP	CAMP:M	Yes / NA	
		3.3.5.10.3.2	SCMS Connectivity Requirement - IEEE Std 1609.2.1	1609.2.1:M	Yes / NA	
2.5.5.10.4	Store Certificates and Associated Private Keys			M	Yes	
		3.3.5.10.4.1	Key Storage Security	M	Yes	
		3.3.5.10.4.2	Certificate Storage Security	M	Yes	
		3.3.5.10.4.3	Secure Platform	M	Yes	
2.5.5.10.5	Download CRLs			M	Yes	
		3.3.5.10.5.1	Download CRL Requirements - CAMP	CAMP:M	Yes / NA	
		3.3.5.10.5.2	Download CRL Requirements – IEEE Std 1609.2.1	1609.2.1:M	Yes / NA	
		3.3.5.10.5.3	Update CRL	M	Yes	
2.5.5.10.6	Download SCMS Files			M	Yes	
		3.3.5.10.6.1	Download SCMS Files - CAMP	CAMP:M	Yes / NA	
		3.3.5.10.6.2	Download SCMS Files – IEEE Std 1609.2.1	1609.2.1:M	Yes / NA	
		3.3.5.10.6.3	Update SCMS Files	M	Yes	
2.5.5.11	Secure Administration			M	Yes	
		3.3.5.11	Secure Administration Requirement	M	Yes	
2.5.5.12	Secure Management of Credentials			M	Yes	
		3.3.5.12.1	Provision of Credentials	M	Yes	
		3.3.5.12.2	Update Credentials	M	Yes	
		3.3.5.12.3	Expiration of Credentials	M	Yes	
2.5.5.13	Logging for General and Security Purposes			M	Yes	
		3.3.5.13	Logging for General and Security Purposes Requirement	M	Yes	
2.5.5.14	Secure Updates			M	Yes	
		3.3.5.14	Secure Update Requirement	M	Yes	
2.5.5.15	Support SCMS for OBUs/MUs			M	Yes	
		3.3.2.5	Network Interface Requirement	M	Yes	
		3.3.4.1	Back-Office Interface Requirement	M	Yes	
		3.3.4.2.2.1	WAVE	M	Yes	
		3.3.4.2.2.3	Internet Protocol	M	Yes	
		3.3.4.2.2.4	WAVE Service Advertisement	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		3.3.4.2.2.5	WAVE Router Advertisement	M	Yes	

3.3 Requirements

The requirements for the RSU follow.

3.3.1 General/Hardware/Mounting Requirements

This section contains requirements regarding the overall RSU device.

3.3.1.1 Power-over-Ethernet Plus (POE+)

The RSU shall be able to function as a Type 2 Powered Device (PD) as defined by IEEE Std 802.3™-2018 Section Two, Clause 33. A Type 2 PD is commonly known as a POE+ device.

3.3.1.2 Environmental Requirements

This section contains the RSU environmental requirements.

3.3.1.2.1 Ambient Temperature RSU

The RSU shall function as intended within the temperature range of -34 degrees C (-30 degrees F) to +74 degrees C (+165 degrees F).

3.3.1.2.2 Ambient Temperature Rate of Change RSU

The RSU shall function as intended under changes in ambient temperature up to 17 degrees C (30 degrees F) per hour, throughout the required operational temperature range.

3.3.1.2.3 Storage Temperature RSU

The RSU shall function as intended after storage at a temperature range of -45 degrees C (-50 degrees F) to +85 degrees C (+185 degrees F).

3.3.1.2.4 Humidity RSU

The RSU shall continuously function under a relative humidity of 95% non-condensing over the temperature range of +4.4 degrees C (+40.0 degrees F) to +43.3 degrees C (+110.0 degrees F). Above +43.3 degrees C (110 degrees F), constant absolute humidity is maintained.

3.3.1.2.5 Rain Resistance Test

The RSU shall pass the rain resistant test using a rainfall rate of 1.7 mm/min (4 in/hour), wind speed of 18 m/sec (40 mph) and 30 minutes on each surface of the device as specified by MIL-STD-810H Method 506.6 Rain, Procedure I - Rain and Blowing Rain.

3.3.1.2.6 Corrosion Resistance Enclosure

The RSU shall continuously function in a corrosion-resistant enclosure that is conformant with the IP67 rating (IEC 60529) or higher.

3.3.1.2.7 Corrosion Resistance Test

The RSU enclosure shall pass the salt fog test with 5% saline exposure for 2 cycles x 48 hours (24 hours wet/24 hours dry) as specified by MIL-STD-810H Method 509.7 Salt Fog.

3.3.1.3 Power Protection and Filtering Requirements

This section contains requirements concerning power protection.

3.3.1.3.1 Transients

The RSU shall conform to IEC 61000-4-4:2012, Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test - Level 2.

3.3.1.3.2 Surges

The RSU shall conform to IEC 61000-4-5:2017, Electromagnetic compatibility (EMC) - Part 4-5: Testing and measurement techniques - Surge immunity test - Level 3.

Note: This is a minimal requirement. Additional external surge protectors are recommended. For antenna wire greater than 10 feet to the antenna port, lightning protection for the antenna is recommended in certain areas.

3.3.1.4 Resistance to Shock and Vibration Requirements

This section contains the shock and vibration requirements for the RSU.

3.3.1.4.1 Vibration

The RSU shall continue its defined functions and maintain physical integrity when subjected to a vibration of 5 to 30 Hz up to 0.5 g applied in each of three mutually perpendicular planes.

3.3.1.4.2 Shock

The RSU shall withstand a shock of 10 g applied in each of three mutually perpendicular planes without suffering any permanent mechanical deformation or damage that renders the unit inoperable.

3.3.1.4.3 Operational Vibration Test

Prior to any other environmental testing (to fulfill the environmental requirements in Section 3.3.1.2, Environmental Requirements), the RSU shall pass the Vibration Test defined in in NEMA TS 2-2016, Section 2.2.8 with the following modifications:

- The test unit shall be operating during the test.

3.3.1.4.4 Non-Operational Shock Test

Prior to any other environmental testing (to fulfill the environmental requirements in Section 3.3.1.2, Environmental Requirements) except satisfactory completion of the vibration test, the RSU shall pass the Shock (Impact) Test defined in NEMA TS 2-2016, Section 2.2.9, with the following modifications:

a) The test unit shall be subjected to a 10G force having a duration of 11 milliseconds.
b) The test shall use a waveform suitable to simulate a drop test (such as sawtooth) with an 11 millisecond rise time and 0 millisecond fall time.
c) The test unit shall be subjected to the test three times in both the positive and negative directions for all three axes.

3.3.1.5 Resistance to Electronic Emissions

The RSU shall conform to requirements for radio frequency (RF)/Electromagnetic Interference (EMI) per IEC 61000-6-2:2016, Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments with a test range to 6 GHz.

3.3.1.6 Out-of-Band and Out-of-Channel Interference Requirements

This section contains out-of-band and out-of-channel interference requirements.

3.3.1.6.1 IEEE Std 802.11 Out-of-Band and Out-of-Channel Interference Requirements

The DSRC V2X interfaces of the RSU shall comply with IEEE Std 802.11 enhanced adjacent and non-adjacent channel rejection (dot11ACRType equal to 2).

3.3.1.6.2 3GPP PC5 Mode 4 (Release 14 or 15) Out-of-Band and Out-of-Channel Interference Requirements

The PC5 V2X interfaces of the RSU shall comply with 3GPP 36.521 (Release 14 or 15). The transmitter and receiver conformance requirements for user equipment (UE) are applied to the RSU.

3.3.1.7 Resistant to Electrostatic Discharge

The RSU shall be able to withstand electrostatic discharges from the air up to +/-15 kiloVolts (kV) or electrostatic discharges on contact up to +/-8 kiloVolts (kV), in conformance with IEC 61000-4-2:2008, Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test.

3.3.1.8 Limit Electronic Emissions Requirements

This section contains electronic emissions requirements.

3.3.1.8.1 Electronic Emissions

The RSU shall require a grant for equipment authorization per CFR Title 47 – Telecommunication, Chapter 1 – Federal Communications Commission, Part 15 and Part 90 (Regulations Governing the Use of Frequencies in the 5850-5925 MHz Band).

3.3.1.8.2 IEEE Std 802.11 Emissions Mask

The DSRC V2X interfaces of the RSU shall comply with IEEE Std 802.11 STA transmit power class: Class C.

3.3.1.8.3 3GPP PC5 Mode 4 (Release 14 or 15) Emissions Mask

The PC5 V2X interfaces of the RSU shall comply with 3GPP 36.521 (Release 14 or 15). The transmitter and receiver conformance requirements for user equipment (UE) are applied to the RSU.

3.3.1.9 Mounting Requirements

This section contains RSU mounting requirements.

3.3.1.9.1 RSU Pole Mounting Requirements

The RSU shall have a configuration that is suitable for mounting on a pole or mast arm.

3.3.1.9.2 RSU Rack Mounting Requirements

The RSU shall have a configuration that is suitable mounting in an electronic equipment rack within a transportation field cabinet.

3.3.1.9.3 RSU Shelf Mounting Requirements

The RSU shall have a configuration that is suitable for mounting on a shelf within a transportation field cabinet.

3.3.1.9.4 RSU Wall Mounting Requirements

The RSU shall have a configuration that is suitable for mounting on a wall within a transportation field cabinet.

3.3.1.10 Diagnostic Testing Requirements

This section contains diagnostic testing requirements.

3.3.1.10.1 Diagnostic Setting – Forwarding Received Messages

The RSU shall have a diagnostic setting when all messages received on the V2X interfaces can be forwarded to the network interface without verifying signatures.

3.3.1.10.2 Diagnostic Setting - Forwarding Transmitted Messages

The RSU shall have a diagnostic setting where all messages transmitted on the V2X interface can be forwarded to the network interface. This requirement supports the user need in NTCIP 1218 v01, 2.5.1.2.2.5 Manage Transmitted Messages over the V2X Interface for Forwarding.

The applicable requirements in NTCIP 1218 v01 are:

- 3.5.1.2.2.4.1 Determine Maximum Number of Message Entries Transmitted Over the V2X Interface for Forwarding Supported
- 3.5.1.2.2.4.2 Store Network Destination to Forward Messages Transmitted Over the V2X Interface
- 3.5.1.2.2.4.3 Store Transport Protocol to Forward Messages Transmitted Over the V2X Interface
- 3.5.1.2.2.4.4 Store Start Time to Forward Messages Transmitted Over the V2X Interface
- 3.5.1.2.2.4.5 Store Stop Time to Forward Messages Transmitted Over the V2X Interface

3.3.1.10.3 Diagnostic Setting - Storing Sent and Received Messages

The RSU shall have a diagnostic setting when all messages sent and received on all interfaces and are stored and can be retrieved.

3.3.1.10.4 Diagnostic Setting – Features Accessible through SNMP

Access to all diagnostic features mandated by this standard shall be fully documented and accessible through the SNMPv3 interface.

3.3.1.10.5 Diagnostic Setting – Transmitting without Signature

The RSU shall have a diagnostic setting when all messages can be transmitted on the V2X interface without the RSU applying signatures to the messages. The message source originates on the RSU or it may originate elsewhere and be received by the RSU and transmitted on the V2X interface.

3.3.1.11 Maintainability Requirements

This section contains RSU maintainability requirements.

3.3.1.11.1 Power Indication Requirements

This section contains power indication requirements for the RSU.

3.3.1.11.1.1 Power Indication

The RSU shall have an external LED to indicate the power status of the device in accordance with the following protocol: Off – No Power and Steady Green – Device is powered on.

3.3.1.11.1.2 Power Indication Location

The power LED shall be located on the RSU's enclosure and be directionally visible from the ground at a reasonable viewing angle when the RSU is mounted in its standard mounting orientation (whether the RSU is inside an opened enclosure or mounted on a pole or a mast arm).

3.3.1.11.1.3 Power LED Characteristics

The power LED shall have the optical characteristics as identified below:

LED Color	Size (mm)	Luminous Intensity (mcd)	Viewing Angle (degrees)
Green	≥ 3	≥ 55	≥ 40

3.3.1.11.2 Status Indication Requirements

This section contains status indication requirements for the RSU.

3.3.1.11.2.1 Status Indication

The RSU shall have external LED indications to show the operational status of the device in accordance with the following protocol: Off – No Power, Blinking Green – Device Start-Up, Steady Green – Device Operational, Amber – Firmware Update in Progress, and Red – Fault.

3.3.1.11.2.2 Status Indication Location

The status LED(s) shall be located on the RSU's enclosure and be directionally visible from the ground at a reasonable viewing angle when the RSU is mounted in its standard mounting orientation (whether its inside an enclosure or mounted on a pole or a mast arm).

3.3.1.11.2.3 Status LED Characteristics

The status LED(s) shall have the optical characteristics as identified below:

Table 10. Status LED Optical Characteristics

LED Color	Size (mm)	Luminous Intensity (mcd)	Viewing Angle (degrees)
Red	≥ 3	≥ 30	≥ 40
Green	≥ 3	≥ 55	≥ 40
Yellow, Orange or Amber	≥ 3	≥ 34	≥ 40

3.3.1.12 Quality Construction Requirements

This section contains quality construction requirements.

3.3.1.12.1 Edges

The RSU shall have all sharp edges and corners rounded and free of burrs.

3.3.1.12.2 Non-Electronic Hardware Materials

Metal non-electric hardware, when used in the construction of the RSU shall be made of non-corrosive material.

3.3.1.12.3 Electrical Isolation and Equipment Grounding

The RSU shall have a minimum transient suppression of 5KA 8/20µs that is terminated to earth ground.

Note: This requirement may be met by adding external surge protection device to the RSU's POE+ Ethernet connection.

3.3.1.12.4 Electrical Installation and Integration

The POE+ power source shall be isolated from other 48 Vdc used in the cabinet.

3.3.1.12.5 Component Operational Requirements

This section contains requirements for RSU components.

3.3.1.12.5.1 Maximum Ratings

No discrete component of the RSU shall be operated above 80 percent of its maximum rated voltage, current or power ratings. For example, a capacitor, resistor or transistor.

3.3.1.12.5.2 PCB Locking Devices

The RSU shall be provided with devices to prevent the PCB from backing out of its assembly connectors. All screw type fasteners shall utilize locking devices or locking compounds except for finger screws, which shall be captive.

3.3.1.12.6 Manufacturer's Specifications

The design of the RSU shall be such that all components are used within the component manufacturer's specifications.

3.3.1.12.7 Enclosure Surface Ultraviolet Protection (Discoloring)

The RSU shall use ultraviolet (UV) protection (a UV-treated surface) on the RSU's external surfaces (enclosure and antenna coverings).

Note: The requirement is also intended to minimize discoloration.

3.3.1.13 Interchangeability Requirements

This section contains RSU interchangeability requirements.

3.3.1.13.1 Ethernet Connector

The RSU shall provide a minimum of 1x100 Base-T Ethernet (8P8C modular jack, commonly known as RJ-45 incorrectly) port that is conformant with IEEE Std 802.3™-2018, including IPv4 and IPv6.

3.3.1.13.2 Powered Connector

The RSU shall use an external 8P8C modular jack (commonly known as RJ-45 incorrectly), CAT-5e connector, with Jack 13/16" - 28 UN screwed in threading that conforms to a minimum Outdoor IP67 rating.

3.3.1.13.3 Antenna Connectors

If the RSU supports interchangeable antennas (including connector port and cabling), then the RSU shall use a Type N connector for the V2X RF antenna, with an impedance of 50 ohms.

Note: For a rack-mounted, shelf-mounted or wall-mounted RSU, additional lightning suppression is recommended for the antenna cable.

3.3.1.13.4 Open Standards

The RSU shall have physical, electrical and communication interfaces based on existing open (i.e., that are obtainable by anyone) standards or defined within this standard.

3.3.1.13.5 Management Information Base

The MIBs necessary for an agency to operate, configure and manage the RSU shall be made available and accessible via SNMPv3.

3.3.1.13.6 Communications Interface

The information necessary for an agency to operate, configure and manage the communications interfaces for the RSU shall be fully documented and made available to the operating agency.

3.3.1.14 Software and Firmware Updates Requirements

The RSU shall support remote software and firmware updates per the requirements of NTCIP 1218 v01. This requirement supports the user need in NTCIP 1218 v01, 2.5.1.1.5 Manage RSU Firmware Version.

The applicable requirements in NTCIP 1218 v01 are:

- 3.5.1.1.5.1 Report the RSU Firmware Version
- 3.5.1.1.5.2 Update the RSU Firmware Version
- 3.5.1.1.5.3 Report Firmware Update Status

Note: Some firmware may not be updateable.

NOTE: The security of the RSU depends on the secure management of the RSU manufacturer software and firmware update signing key, but it is beyond the scope of this document to specify those details. It is expected that protections for the signing key will include being stored in an HSM.

3.3.1.15 Size and Weight Requirements

This section contains RSU size and weight requirements.

3.3.1.15.1 Weight

The RSU shall be less than 6.8 kilograms (15.0 pounds), excluding antennas and mounting brackets.

3.3.1.15.2 Size

The RSU shall have a surface area of less than 5,452 square centimeters (845 square inches), not including antennas and brackets.

3.3.1.16 User Safety Requirements

The RSU shall conform to IEC 62368-1:2018 Annex Y, Hardware Conformance Statement "Installed Outdoor Hardware Safety" and criteria "M".

3.3.2 Functional Requirements

This section identifies the requirements that fulfills the operational needs of an RSU.

3.3.2.1 Startup Requirements

This section contains RSU Startup requirements.

3.3.2.1.1 RSU Startup Functions

The RSU shall retrieve and configure its startup capabilities and functions per the requirements of NTCIP 1218 v01. This requirement supports the user need in NTCIP 1218 v01, 2.5.1.1.4 Manage RSU Startup Functions.

The applicable requirements in NTCIP 1218 v01 are:

- 3.5.1.1.4.2 Manage RSU Startup Functions - Applications
- 3.5.1.1.4.3 Manage RSU Startup Functions - Configuration (Optional)
- 3.5.1.1.4.4 Configure Startup Retries (Optional)
- 3.5.1.1.4.5 Retrieve Startup Retry Period Startup (Optional)

3.3.2.1.2 RSU Restarts

The RSU shall support a startup that reverts to the last saved values of every read-write object described in NTCIP 1218 v01, Section 5, unless explicitly stated otherwise in the object description.

3.3.2.1.3 RSU Transition from Startup

The RSU shall transition out of "startup" mode in less than 120 seconds after a restart.

3.3.2.1.4 Application Configuration

The RSU shall save and restore an application configuration per the requirements of NTCIP 1218 v01. This requirement supports the user need in NTCIP 1218 v01, 2.5.1.4.2 Save and Restore Application Configuration.

The applicable requirements in NTCIP 1218 v01 are:

- 3.5.1.4.2.1 Install a Configuration File
- 3.5.1.4.2.2 Report Configuration File Update Status

3.3.2.2 Restart Requirements

This section contains requirements that satisfy the restart needs of an RSU.

3.3.2.2.1 Remote Restart

The RSU shall support a remote restart that reverts to the last saved values of every read-write object described in NTCIP 1218 V01, Section 5, unless explicitly stated otherwise in the object description. This is a revision of the requirement in NTCIP 1218 v01 is 3.5.3.3, Reboot RSU. The firmware, operating software, configuration settings and log files are retained in memory.

3.3.2.2.2 Factory Settings

The RSU shall support a means to set the RSU back to the factory default locally. It is noted that once an RSU is reset to factory default, the maintenance personnel may have to reconfigure the RSU locally.

3.3.2.2.3 Default Settings

The RSU shall support a means to set the RSU back to a user configured default. This requires the RSU to maintain a set of user-defined value for every object described in a MIB, including the MIB for NTCIP 1218. The firmware, operating software, and log files are retained in memory.

3.3.2.2.4 Log Restarts

The RSU shall log all restart operations in the RSU's event log file.

3.3.2.3 Time Keeping Requirements

This section contains time keeping requirements for an RSU.

3.3.2.3.1 Track Time Requirements

This section contains time tracking requirements for an RSU.

3.3.2.3.1.1 Time Reference

The RSU shall maintain time using UTC as the time of reference.

3.3.2.3.1.2 Time Output

The RSU shall put time in messages and log files in a format conformant to UTC as defined by the International Telecommunications Union Recommendation (ITU-R TF.460-6), Standard-frequency and time-signal emissions.

3.3.2.3.1.3 Time Accuracy - Primary Time Source

The time output from the RSU system clock when using the primary time source shall be accurate to ± 10 milliseconds of the UTC reference.

Note: A PC5 system will likely have its own time source.

3.3.2.3.1.4 Leap Seconds

The RSU shall insert a leap second immediately after the last second of the UTC day specified for the leap second addition. Time source is based on 1970 reference and leap second adjustments.

3.3.2.3.2 Time Source Requirements

This section contains time source requirements for an RSU.

3.3.2.3.2.1 Primary Time Source

The RSU shall use a GNSS receiver as its primary time source.

3.3.2.3.2.2 Report Primary Time Source

The RSU shall report the status of its time source per the requirements of NTCIP 1218 v01. The applicable requirement in NTCIP 1218 v01 is 3.5.2.3.1 Report RSU Clock Source.

3.3.2.3.2.3 Secondary Time Source

The RSU shall use Network Time Protocol (NTP) as a secondary time source. The RSU shall use NTP as the time source if it has not received valid time from the GNSS after 120 seconds. This assumes that NTP has been configured.

3.3.2.3.2.4 Maintain Operations

The RSU shall continue to broadcast messages for a minimum of one minute even when no valid data from the primary time source is available. After 60 seconds, it can stop or continue.

3.3.2.3.2.5 Log Time Failures

The RSU shall write a CRITICAL entry to the System Log if no valid data is received from the primary time source.

The applicable requirements in NTCIP 1218 v01 are:

- 3.5.1.1.7.3.6 Notification - Time Source Loss
- 3.5.2.3.3 Store Allowable RSU Clock Source Timeout (Optional)
- 3.5.2.3.4 Store Allowable RSU Clock Source Queries (Optional)
- 3.6.3.4 Event Log - Notification

3.3.2.3.2.6 Time Source Server

The RSU shall act as a time source for other field devices. Since the RSU is expected to maintain accurate time, this requirement allows the RSU to serve as an accurate time source for other field devices in the transportation field cabinet.

3.3.2.4 Current Location Requirements

This section contains location requirements for an RSU.

3.3.2.4.1 Location Source

The RSU shall report the status of its location source per the requirements of NTCIP 1218 v01. The applicable requirement in NTCIP 1218 v01 is 3.5.2.4.2 Report Positioning Status.

3.3.2.4.2 Report Location

The RSU shall report its position, as latitude, longitude, elevation, and estimated error based on the WGS-84 coordinate system and its reference ellipsoid, per the requirements of NTCIP 1218 v01.

The applicable requirements in NTCIP 1218 v01 are:

- 3.5.2.4.1 Report RSU Location
- 3.5.2.4.5 Report RSU Estimated Location Error (Optional)

3.3.2.4.3 Location Status

The RSU shall report the status of its location information per the requirements of NTCIP 1218 v01. The applicable requirement in NTCIP 1218 v01 is 3.5.2.4.2 Report Positioning Status.

3.3.2.4.4 Log Location Failure – Satellites

The RSU shall write a CRITICAL entry to the System Log if it is not able to acquire a minimum of 4 satellites within 120 seconds after entering the "Operate" state.

3.3.2.5 Network Interface Requirement

The RSU shall provide an Ethernet interface that can be configured on both IPv6 and IPv4 networks, including implementation of NAT64 as defined in IETF RFC 6146 to support IPv6 over the V2X Interface and IPv4 on the Network Interface. The applicable requirement in NTCIP 1218 v01 is 3.5.1.2.1.2, Configure Ethernet Ports.

3.3.2.6 Performance and Data Requirements

This section contains performance and data requirements for an RSU.

3.3.2.6.1 Operational Logging

The RSU shall record salient events in a non-volatile log in accordance with the requirements of NTCIP 1218 v01. This requirement supports the user need in NTCIP 1218 v01, 2.4.2 Provide for Log Data Local Storage and Retrieval.

The applicable requirements in NTCIP 1218 v01 are:

- 3.4.2.3 Retrieve Event Logged Data
- 3.6.3.1 Event Log - System Events
- 3.6.3.2 Event Log - Application Events
- 3.6.3.3 Event Log - RSU Configuration
- 3.6.3.4 Event Log - Notification
- 3.6.3.5 Event Log - Security
- 3.6.3.6 Event Log - Stored Messages
- 3.6.3.7 Event Log - Immediate Forward Message

3.3.2.6.2 Statistical Data Requirements

This section contains statistical data requirements about V2X messages exchanged by an RSU.

3.3.2.6.2.1 Log Interface Data

The RSU shall log the data sent to and received from V2X devices per the requirements of NTCIP 1218 v01. This requirement supports the user need in NTCIP 1218 v01, 2.5.1.2.3 Manage Logging of Interface Data.

The applicable requirements in NTCIP 1218 v01 are:

- 3.5.1.2.3.2 Log Interface Data Identification
- 3.5.1.2.3.3 Log Interface Data by Direction (Optional)
- 3.5.1.2.3.4 Store Interface Data Log - File Directory (Optional)
- 3.5.1.2.3.5 Retrieve Interface Logged Data
- 3.5.1.2.3.6 Store an Interface Data Log Start Time (Optional)
- 3.5.1.2.3.7 Store an Interface Data Log Stop Time (Optional)
- 3.5.1.2.3.8 Store Maximum Interface Data Log File Size (Optional)
- 3.5.1.2.3.9 Store Maximum Interface Data Log File Collection Time (Optional)
- 3.5.1.2.3.10 Store Interface Data Log Option - Disk Full (Optional)
- 3.5.1.2.3.11 Store Interface Data Log Option - Entry Deletion (Optional)

3.3.2.6.2.2 Log RF Communications Reception Coverage

The RSU shall report the RF reception coverage using the parameters described in NTCIP 1218 v01. This requirement supports the user need in NTCIP 1218 v01, 2.5.2.8 Determine RF Communications Range.

The applicable requirements in NTCIP 1218 v01 are:

- 3.5.2.8.2 Report the RF Communications Distance - 1 Minute (Optional)
- 3.5.2.8.3 Report the RF Communications Distance - 5 Minutes (Optional)
- 3.5.2.8.4 Report the RF Communications Distance - 15 Minutes (Optional)
- 3.5.2.8.5 Report the Average RF Communications Distance - 1 Minute (Optional)
- 3.5.2.8.6 Report the Average RF Communications Distance - 5 Minutes (Optional)
- 3.5.2.8.7 Report the Average RF Communications Distance - 15 Minutes

3.3.2.6.2.3 Report Number of Messages Exchanged by the V2X Radio

The RSU shall report the number of messages transmitted and received by the V2X radio per the requirements of NTCIP 1218 v01. The applicable requirement in NTCIP 1218 v01 is 3.5.2.6, Report Number of Messages Exchanged by V2X Radio and PSID.

3.3.2.7 RSU Clustering Requirements

This section contains RSU clustering requirements for RSUs. These requirements are not applicable for C-V2X because there is no channel set up scenario at this time.

3.3.2.7.1 RF Bandwidth Support Requirements - DSRC

An RSU typically has two radios. Two radios may not provide enough capacity to support all the applications. One of the radios may be operating in alternating mode, switching between the control channel (CCH) and a service channel (SCH). For example, the service advertised by the RSU is used to provide IPv6 connectivity to OBUs for access to the SCMS or an over-the-air (OTA) update server. The RSU sends a corresponding WSA/WRA on the CCH during time slot 0, then switches to the SCH for time slot 1 in order to provide the service.

This limits the bandwidth for that service to less than half of the possible bandwidth when compared to continuous radio operation. This limitation does not apply to an OBU which can tune one of its radios to the service channel in continuous mode once it has received the WSA / WRA information.

Using additional “service” RSUs which exclusively operate their radios in continuous mode on a service channel this limitation can be overcome by configuring the “advertising” RSU as well as the “service” RSUs appropriately using NTCIP 1218 v01 features. This section identifies the requirements that satisfy this feature.

3.3.2.7.1.1 Configure Radio as a Service RSU

The RSU shall be configured as a "service" RSU. Service channels on an RSU can be configured in continuous mode per the requirements of NTCIP 1218 v01. This applicable requirement in NTCIP 1218 v01 is 3.5.1.3.1, Configure Radio Requirements. Note: The primary RSU has its WSA configured that points to a V2X Interface on the service RSU.

Note: This requirement assumes the RSU has more than one radio. It further assumes that multiple DSRC channels are available for use.

3.3.2.8 Message Handling Requirements

This section contains message handling requirements for an RSU.

3.3.2.8.1 Message Sent by the RSU Requirements

This section contains requirements for V2X messages sent by an RSU.

3.3.2.8.1.1 Signing and Forwarding of Messages Not Signed by the Message Source

For unsigned messages received on the network interface, the RSU shall sign and forward them to the V2X interface per the requirements of NTCIP 1218 v01. This requirement supports the user need in NTCIP 1218 v01, 2.5.1.2.2.3 Manage Received Messages for Forwarding to the V2X Interface. The message is signed according to the IEEE Std 1609.2™-2016 security profile for the corresponding PSID and transmitted as a WSM. The SNMP objects are provisioned according to NTCIP 1218 v01 Section 5.5.

The applicable requirements in NTCIP 1218 v01 are:

- 3.5.1.2.2.2.1 Determine Maximum Number of Immediate Forward Messages Supported
- 3.5.1.2.2.2.2 Forward Message to the V2X Interface
- 3.5.1.2.2.2.3 Store the Message Type for a Message for Forwarding to the V2X Interface
- 3.5.1.2.2.2.4 Store the PSID for an Application Data Exchange for Forwarding to the V2X Interface
- 3.5.1.2.2.2.5 Store the Priority for a Message for Forwarding to the V2X Interface (Optional)
- 3.5.1.2.2.2.6 Store the Transmission Channel for a Message for Forwarding to the V2X Interface
- 3.5.1.2.2.2.7 Store if a Received Message for Forwarding to the V2X Interface is Signed

3.3.2.8.1.2 Forwarding of Messages Signed by the Message Source

The RSU shall forward signed messages received on the network interface to the V2X interface per the requirements of NTCIP 1218 v01. This requirement supports the user need in NTCIP 1218 v01, 2.5.1.2.2.3 Manage Received Messages for Forwarding to the V2X Interface. Using SNMP objects defined in NTCIP 1218 v01, the signed message is transmitted as a WSM. The SNMP objects are provisioned according to NTCIP 1218 Section 5.5.

The applicable requirements in NTCIP 1218 v01 are:

- 3.5.1.2.2.2.1 Determine Maximum Number of Immediate Forward Messages Supported
- 3.5.1.2.2.2.2 Forward Message to the V2X Interface
- 3.5.1.2.2.2.3 Store the Message Type for a Message for Forwarding to the V2X Interface
- 3.5.1.2.2.2.4 Store the PSID for an Application Data Exchange for Forwarding to the V2X Interface
- 3.5.1.2.2.2.5 Store the Priority for a Message for Forwarding to the V2X Interface (Optional)
- 3.5.1.2.2.2.6 Store the Transmission Channel for a Message for Forwarding to the V2X Interface
- 3.5.1.2.2.2.7 Store if a Received Message for Forwarding to the V2X Interface is Signed

3.3.2.8.1.3 Storing and Repeating Messages Not Signed by the Message Source

The RSU shall sign, store and periodically repeat unsigned messages received on the network interface to the V2X interface per the requirements of NTCIP 1218 v01. This requirement supports the user needs in NTCIP 1218 v01 2.5.1.2.2.1 Manage Stored Messages, and 2.5.1.2.2.2 Manage Stored Messages for Transmission. Using SNMP objects defined in NTCIP 1218, the message is signed and certificate attached according to the security profile for the corresponding PSID and transmitted periodically as a WSM. The SNMP objects are provisioned according to NTCIP 1218 section 5.4.

The applicable requirements in NTCIP 1218 v01 are:

- 3.5.1.2.2.1.1 Determine Maximum Number of Stored Messages Supported
- 3.5.1.2.2.1.2 Store a Message
- 3.5.1.2.2.1.3 Delete a Stored Message
- 3.5.1.2.2.1.4 Enable/Disable the Transmission of a Stored Message
- 3.5.1.2.2.1.5 Store a Message Type
- 3.5.1.2.2.1.6 Store PSID for Application Data Exchanges
- 3.5.1.2.2.1.7 Delete All Stored Messages (Optional)
- 3.5.1.2.2.1.8 Store a Message's Priority
- 3.5.1.2.2.1.9 Store a Message's Transmission Interval
- 3.5.1.2.2.1.10 Store a Message's Transmission Channel
- 3.5.1.2.2.1.11 Store a Message's Transmission Start Time
- 3.5.1.2.2.1.12 Store a Message's Transmission Stop Time
- 3.5.1.2.2.1.13 Store if a Message is to be Signed

3.3.2.8.1.4 Storing and Repeating Messages Signed by the Message Source

The RSU shall store and periodically repeat signed messages received on the network interface to the V2X interface per the requirements of NTCIP 1218 v01. This requirement supports the user needs in NTCIP 1218 v01 2.5.1.2.2.1 Manage Stored Messages, and 2.5.1.2.2.2 Manage Stored Messages for Transmission. Using SNMP objects defined in NTCIP 1218, the message is transmitted periodically as a WSM. The SNMP objects are provisioned according to NTCIP 1218 section 5.4.

The applicable requirements in NTCIP 1218 v01 are:

- 3.5.1.2.2.1.1 Determine Maximum Number of Stored Messages Supported
- 3.5.1.2.2.1.2 Store a Message
- 3.5.1.2.2.1.3 Delete a Stored Message
- 3.5.1.2.2.1.4 Enable/Disable the Transmission of a Stored Message
- 3.5.1.2.2.1.5 Store a Message Type
- 3.5.1.2.2.1.6 Store PSID for Application Data Exchanges
- 3.5.1.2.2.1.7 Delete All Stored Messages (Optional)
- 3.5.1.2.2.1.8 Store a Message's Priority
- 3.5.1.2.2.1.9 Store a Message's Transmission Interval
- 3.5.1.2.2.1.10 Store a Message's Transmission Channel
- 3.5.1.2.2.1.11 Store a Message's Transmission Start Time
- 3.5.1.2.2.1.12 Store a Message's Transmission Stop Time
- 3.5.1.2.2.1.13 Store if a Message is to be Signed

3.3.2.8.2 Forwarding of Messages Received by the RSU

The RSU shall forward messages received on the V2X interface to the RSCE, TMS or the back-office system per the requirements of NTCIP 1218 v01. Using a PSID to UDP port number mapping, the relevant message is verified and forwarded to the UDP port number on the network interface, according to the SNMP objects defined in NTCIP 1218. The SNMP objects are provisioned according to NTCIP 1218 section 5.6. An implementation of V2X message forwarding that forwards all WSMs without the ability to specify PSIDs for forwarding would not meet this requirement.

The applicable requirements in NTCIP 1218 v01 are:

- 3.5.1.2.2.3.1 Determine Maximum Number of Message Received Types Supported
- 3.5.1.2.2.3.2 Store Network Destination to Forward Messages Received from the V2X Interface
- 3.5.1.2.2.3.3 Store Transport Protocol to Forward Messages Received from the V2X Interface (Optional)
- 3.5.1.2.2.3.4 Store Minimum Signal Strength to Forward Messages Received from the V2X Interface (Optional)
- 3.5.1.2.2.3.5 Store Message Interval to Forward Messages Received from the V2X Interface (Optional)
- 3.5.1.2.2.3.6 Store Start Time to Forward Messages Received from the V2X Interface
- 3.5.1.2.2.3.7 Store Stop Time to Forward Messages Received from the V2X Interface
- 3.5.1.2.2.3.8 Enable/Disable Forwarding Messages Received from the V2X Interface
- 3.5.1.2.2.3.9 Store Secure Options to Forward Messages Received from the V2X Interface (Optional)
- 3.5.1.2.2.3.10 Store Interval to Authenticate Messages Received from the V2X Interface (Optional)

3.3.2.8.3 Message Transfer Latency

This section contains message transfer latency requirements for an RSU.

3.3.2.8.3.1 Time Critical Messages

For time-critical messages the latency between reception on one interface (V2X or network interface) and transmission on the other interface on the same RSU (V2X or network interface) shall be less than 50 milliseconds (including signing if necessary). Time critical messages correspond to the applications shown in Table 11. For DSRC, this should be tested when the RSU is operating in continuous mode.

Table 11. Latency - Time Critical Messages

PSID	Application	Reference Feature Design Section
0x82, (0p82)	intersection safety and awareness (i.e. SPaT)	4.3.2.14.1
0x20-40-95, (0pE0-00-00-15)	Traffic signal priority / preemption (SSM - status)	
0x20-40-96, (0pE0-00-00-16)	Traffic signal priority / preemption (SRM - request)	

3.3.2.8.3.2 Non-Time Critical Messages

For non-time critical messages (all other applications), latency between reception on one interface (V2X or network interface) and transmission on the other interface (V2X or network interface) shall be less than 1 second.

3.3.2.9 Application Requirements

This section contains requirements regarding the applications of an RSU.

3.3.2.9.1 SPaT Processing Requirements

This section contains SPaT processing requirements for an RSU.

3.3.2.9.1.1 NTCIP 1202

The RSU shall encode (UPER), sign and broadcast SPaT messages upon receiving SPaT information in NTCIP 1202 v03A format from the TSC.

3.3.2.9.1.2 TSCBM

The RSU shall encode (UPER), sign and broadcast SPaT messages upon receiving SPaT information in TSCBM format from the TSC.

3.3.2.9.2 BSM Processing Requirements

This section contains BSM processing requirements for an RSU.

3.3.2.9.2.1 BSM Filtering

The RSU shall forward the first BSM received from each vehicle traveling into a specific zone. The zone criteria are defined geographically and based on heading. A minimum of 4 zones can be defined per RSU, and BSMs are forwarded if the zone criteria are met. Zones can be established to support safety (e.g., wrong way driver) and mobility (e.g., travel time) applications as well as RF coverage performance.

BSMs that meet the criteria are forwarded using the interface in Section 3.3.2.8.2.

3.3.3 Behavioral Requirements

This section contains the configuration, management and monitoring requirements for an RSU.

3.3.3.1 Configuration and Management Requirements

This section contains configuration requirements for an RSU.

3.3.3.1.1 Retrieve RSU Identity

The RSU shall provide its identifier per the requirements of NTCIP 1218 v01.

The applicable requirements in NTCIP 1218 v01 are:

- 3.5.1.1.1.1 Store RSU Identifier
- 3.5.1.1.1.2 Report RSU Component Information
- 3.5.1.1.1.3 Report Supported Standards (Optional)
- 3.5.1.1.1.4 Report RSU System Name
- 3.5.1.1.1.5 Report RSU MIB Version (Optional)

3.3.3.1.2 Retrieve Configuration Version of the RSU

The RSU shall provide the version of the configuration parameters for the RSU per the requirements of NTCIP 1218 v01. This applicable requirement in NTCIP 1218 v01 is 3.5.1.1.2 Report Deployment Configuration Identifier.

3.3.3.1.3 Configure RSU Location

The RSU shall set its reference location (latitude, longitude, and elevation) per the requirements of NTCIP 1218 v01. The reference location is used for fixed-location RSUs and may be based on high resolution mapping. This requirement supports the user need in NTCIP 1218 v01, 2.5.1.1.3 Manage RSU Location Information.

The applicable requirements in NTCIP 1218 v01 are:

- 3.5.1.1.3.1 Store RSU Location Description (Optional)
- 3.5.1.1.3.2 Store RSU Location
- 3.5.1.1.3.3 Store RSU Location - GNSS Antenna Offset (Optional)
- 3.5.1.1.3.4 Store V2X Antenna Offsets (Optional)

3.3.3.1.4 Notifications

The RSU shall configure notifications per the requirements of NTCIP 1218 v01. This requirement supports the user need in NTCIP 1218 v01, 2.5.1.1.7 Manage Notifications.

The applicable requirements in NTCIP 1218 v01 are:

- 3.5.1.1.7.1 Store Notification Destination Address
- 3.5.1.1.7.2 Store Notification Destination Port
- 3.5.1.1.7.3.1 Notification - Integrity Check Error - Active Message
- 3.5.1.1.7.3.2 Notification - Integrity Check Error - Secure Storage
- 3.5.1.1.7.3.3 Notification - Authorization Verification Error
- 3.5.1.1.7.3.4 Notification - Signature Verification Error
- 3.5.1.1.7.3.5 Notification - Network Access Control List
- 3.5.1.1.7.3.6 Notification - Time Source Loss
- 3.5.1.1.7.3.7 Notification - Time Source Mismatch
- 3.5.1.1.7.3.8 Notification - GNSS Anomaly
- 3.5.1.1.7.3.9 Notification - GNSS Location Deviation
- 3.5.1.1.7.3.10 Notification - Certificate Management
- 3.5.1.1.7.3.11 Notification - Denial of Service (Optional)
- 3.5.1.1.7.3.12 Notification - Watchdog (Optional)
- 3.5.1.1.7.3.13 Notification - GNSS Data (Optional)
- 3.5.1.1.7.3.14 Notification - Configure GNSS Data Interval (Optional)
- 3.5.1.1.7.3.15 Notification - Environmental (Optional)
- 3.5.1.1.7.3.16 Notification - Authentication Failure
- 3.5.1.1.7.4 Store Notification Type (Optional)
- 3.5.1.1.7.5 Store Notification Repeat Intervals (If Store Notification Type is supported)
- 3.5.1.1.7.6 Store Notification Retries (If Store Notification Type is supported)

3.3.3.1.5 Configuration Error Resilience

The RSU shall continue to operate and respond to NTCIP 1218 requests after processing valid as well as invalid NTCIP 1218 requests. Note: The purpose of this requirement is to verify and assist in ensuring that the RSU does not enter an unresponsive state simply from processing NTCIP requests. The expectation is that the RSU accepts all valid requests per NTCIP 1218 specification as well as responds with an appropriate error to invalid requests.

3.3.3.1.6 Control Mode of Operation

The RSU shall control the mode of operations per the requirements of NTCIP 1218 v01. The applicable requirement in NTCIP 1218 v01 is 3.5.3.1 Control Mode of Operation.

3.3.3.1.7 Control RF Antenna Output

The RSU shall set the transmit power of a RF channel per the requirements of NTCIP 1218 v01. The applicable requirement in NTCIP 1218 v01 is 3.5.3.2, Control RF Antenna Output. The transmit power should account for antenna gain and cable loss factors.

3.3.3.1.8 Control Application

The RSU shall enable or disable a resident application per the requirements of NTCIP 1218 v01. The applicable requirement in NTCIP 1218 v01 is 3.5.3.4, Control Application.

3.3.3.2 Health and Status Monitoring Requirements

This section contains health and status monitoring requirements for an RSU.

3.3.3.2.1 Determine Mode of Operations

The RSU shall report its current mode of operations per the requirements of NTCIP 1218 v01. The applicable requirement in NTCIP 1218 v01 is 3.5.2.2, Report Mode of Operations.

3.3.3.2.2 Monitor Current Status

The RSU shall report its operational status per the requirements of NTCIP 1218 v01. There are a set of requirements in NTCIP 1218 that provide a comprehensive picture of the current operational status of the RSU.

The applicable requirements in NTCIP 1218 v01 are:

- 3.5.1.3.3.1.1 Report IEEE Std 1609.2 Enrollment Certificate - Status
- 3.5.1.3.3.1.7 Report IEEE Std 1609.2 Application Certificates - Status
- 3.5.1.3.1.5 Report Radio Operating Modes
- 3.5.2.2 Report Mode of Operations
- 3.5.2.3.1 Report RSU Clock Source
- 3.5.2.3.2 Report RSU Clock Status
- 3.5.2.11.1 Report RSU Current Overall Status
- 3.5.2.11.2.1 Report RSU System Services Status

3.3.3.2.3 Determine Operational Performance

The RSU shall report operational performance statistics of the RSU per the requirements of NTCIP 1218 v01. This requirement supports the user need in NTCIP 1218 v01, 2.5.2.1 Determine RSU Operational Performance Status.

The applicable requirements in NTCIP 1218 v01 are:

- 3.5.2.1.1 Report Time Elapsed Since RSU Power On
- 3.5.2.1.2 Report Amount of Free Memory (Optional)
- 3.5.2.1.3 Report Instantaneous CPU Load (Optional)
- 3.5.2.1.4 Report CPU Load Average - 15 Minutes (Optional)
- 3.5.2.1.5 Report CPU Load Average - 5 Minutes (Optional)
- 3.5.2.1.6 Report CPU Load Average - 1 Minute (Optional)
- 3.5.2.1.7 Report Storage Space Available (Optional)
- 3.5.2.1.8 Report Number of Messages Exchanged (Optional)

3.3.3.2.4 Determine Operating Environment

The RSU shall report the operating environment inside the RSU enclosure per the requirements of NTCIP 1218 v01. This requirement supports the user need in NTCIP 1218 v01, 2.5.2.10 Determine RSU Environment.

The applicable requirements in NTCIP 1218 v01 are:

- 3.5.2.10.1 Report the Internal Operating Temperature
- 3.5.2.10.2 Determine the Internal Operating Temperature Thresholds (Optional)

3.3.3.3 Visual Indications Requirements

This section contains visual indication requirements for an RSU.

The applicable requirements are found in Section 3.3.1.11.

3.3.4 Interface Requirements

This section contains the interface requirements for an RSU.

3.3.4.1 Back-Office Interface Requirement

The RSU shall manage the back-office interface per the requirements of NTCIP 1218 v01. This requirement supports the user need in NTCIP 1218 v01, 2.5.1.2 Manage a Network Interface.

The applicable requirements in NTCIP 1218 v01 are:

- 3.5.1.2.1.1 Enable/Disable a Communications Port
- 3.5.1.2.1.2 Configure Ethernet Port
- 3.5.1.2.1.3 Report Ethernet Port - MAC Address

3.3.4.2 V2X Interface Requirements

This section contains the V2X Interface requirements for an RSU.

3.3.4.2.1 Lower Layers and Radio Interfaces

This section contains the lower layer and radio interface requirements for the V2X Interface of an RSU.

3.3.4.2.1.1 Transmit Power Requirements

This section contains the transmit power requirements for an RSU.

3.3.4.2.1.1.1 Transmit Power Range and Accuracy

The transmit power out of the V2X radio subsystem as measured at the antenna connector of the subsystem housing shall be within 2 dB of its setting over 95% of measurements at each setting within the range 0 to 20 dBm.

3.3.4.2.1.1.2 Transmit Power Monotonicity

The transmit power out of the V2X radio subsystem measured at the antenna connector of the subsystem housing shall be a monotonically increasing function of the transmit power setting in step sizes of 1 dB over the range 0 to 20 dBm.

3.3.4.2.1.2 DSRC Requirements

This section contains the Dedicated Short-Range Communications (DSRC) requirements for an RSU.

3.3.4.2.1.2.1 DSRC (IEEE Std 802.11)

The RSU shall implement IEEE Std 802.11™-2020 (operating outside the context of a BSS) in the 5.855 to 5.925 GHz band on channels 172, 174, 176, 178, 180. 182 and 184 with 10 MHz channel spacing.

3.3.4.2.1.2.2 Receiver Sensitivity (DSRC)

The packet error rate of the DSRC radio subsystem shall be 10% or less when the PSDU length is 400 octets and the input level is -92 dBm at 6 Mbps (QPSK with 1/2 rate coding), at room temperature (21 degrees C ± 5 degrees C). The minimum input levels are measured at the antenna connector of the RSU.

3.3.4.2.1.2.3 Multi-Channel Operations

For IEEE Std 802.11 Radio Interfaces, the RSU shall implement IEEE Std 1609.4™-2016, according to the SNMP objects defined in NTCIP 1218 v01. The SNMP objects are provisioned according to NTCIP 1218 v01 Section 5.2. The applicable requirement in NTCIP 1218 v01 is 3.5.1.3.3.3 Configure IEEE Std 1609.4 Communications Requirements.

The minimum completed Protocol implementation Conformance Statement (PICS) is in Annex B.3, IEEE Std 1609.4 PICS.

Note: Support for immediate access implies the availability of a second radio operating in continuous mode on the corresponding service channel. See the PICs.

3.3.4.2.1.2.4 Maintain Channel Switching Operations

The RSU shall maintain the current operating (e.g., channel switching in the case of DSRC) mode for a minimum of one minute even when no valid data from the primary time source is available. After 60 seconds, it can stop or continue.

3.3.4.2.1.3 C-V2X Requirements

This section contains the C-V2X requirements for an RSU.

3.3.4.2.1.3.1 C-V2X (3GPP PC5 Mode 4 (Release 14 or 15)) - Channel 183

The RSU shall implement 3GPP PC5 Mode 4 (V2X Sidelink) in the 5.905 to 5.925 GHz band. See SAE J3161 for guidance on configuring the PC5 interface.

3.3.4.2.1.3.2 C-V2X (3GPP PC5 Mode 4 (Release 14 or 15)) - Channel 180

The RSU shall implement 3GPP PC5 Mode 4 (V2X Sidelink) in the 5.895 to 5.905 GHz band. See SAE J3161 for guidance on configuring the PC5 interface.

3.3.4.2.1.3.3 Receiver Sensitivity (C-V2X)

The packet error rate of the PC5 Radio Subsystem shall be 10% or less when the payload length is 367 octets and the input level is -94 dBm using MCS 11, at room temperature (21 degrees C +/- 5 degrees C). This is for a single antenna configuration and using HARQ (one retransmission). For other MCS, the sensitivity level is to be within 6 dB of this figure. The minimum input levels are measured at the antenna connector of the RSU.

3.3.4.2.2 Network and Transport Layer Requirements

This section contains the network and transport layer requirements for the V2X Interface of an RSU.

3.3.4.2.2.1 WAVE

The RSU shall implement IEEE Std 1609.3™-2020. The minimum completed PICS is in Annex B.2, IEEE Std 1609.3 PICS.

3.3.4.2.2.2 WAVE Short Message Protocol

The RSU shall implement the WAVE Short Message Protocol as defined in IEEE Std 1609.3™-2020.

3.3.4.2.2.3 Internet Protocol

The RSU shall implement the IPv6 as defined in IEEE Std 1609.3™-2020.

3.3.4.2.2.4 WAVE Service Advertisement

The RSU shall implement the WAVE Service Advertisement as defined in IEEE Std 1609.3™-2020, according to the SNMP objects defined in NTCIP 1218. The SNMP objects are provisioned according to NTCIP 1218 v01, Section 5.10. The applicable requirement in NTCIP 1218 v01 is 3.5.1.3.3.2, Configure IEEE Std 1609.3 Communications - WSA Requirements.

3.3.4.2.2.5 WAVE Router Advertisement

The RSU shall implement the WAVE Router Advertisement as defined in IEEE Std 1609.3™-2020, according to the SNMP objects defined in NTCIP 1218 v01. The SNMP objects are provisioned according to NTCIP 1218 v01, Section 5.11. The applicable requirement in NTCIP 1218 v01 is 3.5.1.3.3.2.4, Configure WSA Configuration - WAVE Router Advertisement.

3.3.5 Security Requirements

This section contains the security requirements for an RSU.

3.3.5.1 V2X Interface Security Requirements

This section contains the security requirements for exchanging messages across the V2X interface.

3.3.5.1.1 V2X Interface Security - Sending Messages

The RSU shall fulfill the requirements as specified in a completed Protocol implementation Conformance Statement (PICS) for IEEE Std 1609.2b™-2019 in Annex B.1 - IEEE Std 1609.2 PICS.

3.3.5.1.2 V2X Interface Security - Receiving and Forwarding Messages

If the RSU is configured to forward the messages it receives from OBUs/MUs over the V2X Interface, the RSU shall verify the IEEE Std 1609.2b™-2019 signatures of those messages.

3.3.5.2 Local and Back-Office Interface Security Requirements

The RSU shall utilize TLS v1.3, as defined in IETF RFC 8446, to protect all communications between the RSU and local devices (other devices in the TFCS) or back-office devices, with the exception that if a standardized interaction explicitly identified in this standard does not support the use of TLS 1.3 then a different security protocol shall be used for that interaction.

Note: Examples of standardized interaction include SNMP v3. All standardized interactions that may use a security protocol other than TLS v1.3 are identified in Section 4.3.5.11.

3.3.5.3 Manage Data Integrity Requirements

This section contains the data integrity requirements for an RSU.

3.3.5.3.1 Data Integrity - At Rest

The RSU shall protect the integrity of data stored on it per the requirements of NTCIP 1218 v01. The applicable requirement in NTCIP 1218 v01 is 3.6.1.2.1 Access RSU – USM. The RSU verifies that the content of the data is unchanged when stored.

3.3.5.3.2 Data Integrity - In Transit

The RSU shall protect the integrity of data exchanged per the requirements of NTCIP 1218 v01. The applicable requirement in NTCIP 1218 v01 is 3.6.1.2.1 Access RSU - USM. The RSU verifies that the data contents when transmitted are the same as when received and are not corrupted and used in a way it was not intended to.

3.3.5.3.3 Device Integrity - Notification

The RSU shall detect and notify its traffic management system (TMS) per the requirements of NTCIP 1218 v01. This requirement supports the user need in NTCIP 1218 v01, 2.6.2 Manage Data Integrity.

The applicable requirements in NTCIP 1218 v01 are:

- 3.5.1.1.7.3.1 Notification - Integrity Check Error - Active Message
- 3.5.1.1.7.3.2 Notification - Integrity Check Error - Secure Storage

3.3.5.4 Availability Requirements

This section contains availability requirements for an RSU.

3.3.5.4.1 Manage Availability Requirements

The RSU shall support availability functions per the requirements of NTCIP 1218 v01. This requirement supports the user need in NTCIP 1218 v01, 2.6.3 Manage Availability.

The applicable requirements in NTCIP 1218 v01 are:

- 3.5.4.2.1 Report Expiration Date - Enrollment Certificates
- 3.5.4.2.2 Report Expiration Date - Application Certificates

3.3.5.4.2 Device Auditing Requirements

The RSU shall support detecting and reporting an unauthorized access attempt per the requirements of NTCIP 1218 v01. This requirement supports the user need in NTCIP 1218 v01, 2.6.3 Manage Availability. The applicable requirement in NTCIP 1218 v01 is 3.5.1.1.7.3.5 Notification - Network Access Control List.

3.3.5.5 Data Confidentiality Requirements

The RSU shall support data confidentiality functions per the requirements of NTCIP 1218 v01. This requirement supports the user need in NTCIP 1218 v01, 2.6.4 Manage Confidentiality.

The applicable requirements in NTCIP 1218 v01 are:

- 3.6.1.2.1 Access RSU - USM
- 3.6.1.2.2 Access RSU - TSM
- 3.6.1.2.3 Support AES-256 Encryption

3.3.5.6 Tamper Evident Requirements

This section contains requirements for providing tamper evident mechanisms for an RSU.

3.3.5.6.1 Tamper Evident Enclosure - Visual Requirements

The RSU enclosure shall provide tamper evident mechanisms such that a trained operator/maintainer can determine via visual inspection whether an RSU enclosure was breached.

3.3.5.6.2 Tamper Evident Unused Port Requirements

The RSU shall provide tamper evident mechanisms for unused external interfaces (other than RF ports) such that a trained operator/maintainer can determine via visual inspection if unused RSU external interfaces were breached.

3.3.5.6.3 Tamper Evident Enclosure - Bootup Requirements

The RSU shall support a tamper detection mechanism for opening the RSU enclosure while RSU is without power. Upon detection of enclosure opening and powering up, the RSU shall reset itself to factory settings including zeroization of any private keys and identification certificates (e.g., TLS certificates).

3.3.5.7 Private Key Storage Requirements

The RSU shall store all private keys in a security module in accordance with the CAMP Platform Security Document. This requirement applies to non-SCMS related keying material.

3.3.5.8 RSU Operating System Security Requirements

This section contains the RSU Operating System security requirements for an RSU.

3.3.5.8.1 RSU OS Applications and Services

The RSU shall disable, by default, any applications and services within its operating system that are not being utilized.

3.3.5.8.2 RSU OS Ports and Protocols

The RSU shall disable or allow by exception, by default, any ports and protocols not being utilized by any of the active applications running on the RSU.

3.3.5.8.3 RSU Password

The RSU shall prompt the first user to access it to change the default password to a password that meets current password strength requirements.

3.3.5.9 Connection Assurance Requirements

This section contains the network connection assurance requirements for an RSU.

3.3.5.9.1 Assurance of Correct Connection Requirement

The RSU shall be able to gain assurance when it connects to another local device or backend device in its network, that it is being accessed by that device as intended by the administrator of the RSU.

3.3.5.9.2 Assurance of Continued Correct Connection Requirement

The RSU shall be able to gain assurance that any ongoing network connection only allows access from the device it was originally connected to.

3.3.5.10 SCMS Requirements

This section contains the requirements for an RSU to interface with an SCMS.

There are currently two proposed methods for interfacing with an SCMS.

a) At the time this standard was published, the existing interface is defined in the *CAMP CV Pilots Documentation* material.

b) IEEE Std 1609.2.1™-2020, IEEE Standard for Wireless Access in Vehicular Environments--Certificate Management Interfaces for End-Entities, is a recently published standard defining methods to interface with an SCMS and is expected to be used for future implementations. However, at the time this standard was published, no existing implementation are using this interface.

Thus, the requirements for the CAMP document (CAMP) are defined to support near term implementations, while the requirements using IEEE Std 1609.2.1™-2020 are defined to support longer term implementations. An implementation may decide to support both methods if desired.

3.3.5.10.1 SCMS Enrollment Requirements

This section contains requirements for an RSU to enroll with an SCMS.

3.3.5.10.1.1 SCMS Enrollment Requirement - Bootstrapping

The RSU shall undergo a secure bootstrapping process in order to be provisioned with initial SCMS trust material.

3.3.5.10.1.2 SCMS Enrollment Requirement - CAMP

The RSU shall be capable of securely enrolling with an IOO-approved SCMS in accordance with the requirements in the *CAMP CV Pilots Documentation* material. In addition, the RSU shall be capable of re-enrolling with the same approved SCMS.

3.3.5.10.1.3 SCMS Enrollment Requirement - IEEE Std 1609.2.1

The RSU shall be capable of securely enrolling with an IOO-approved SCMS in accordance with IEEE Std 1609.2.1™-2020. In addition, the RSU shall be capable of re-enrolling with the same approved SCMS.

3.3.5.10.2 SCMS Configurability Requirement

The RSU shall be configured for SCMS interaction, in order to be provisioned with the set of applications the RSU requests certificates for and the timing of these requests.

3.3.5.10.3 SCMS Connectivity Requirements

This section contains requirements for an RSU to connect with an SCMS.

3.3.5.10.3.1 SCMS Connectivity Requirement - CAMP

The RSU shall connect to the SCMS via secure methods to request and download new application certificates in accordance with the *CAMP CV Pilots Documentation* material.

3.3.5.10.3.2 SCMS Connectivity Requirement - IEEE Std 1609.2.1

The RSU shall connect to the SCMS via secure methods to request and download new application certificates in accordance with IEEE Std 1609.2.1™-2020.

3.3.5.10.4 Certificate and Private Key Storage Requirements

This section contains requirements for an RSU to store certificates and other cryptographic material with an SCMS.

3.3.5.10.4.1 Key Storage Security

The RSU shall store all SCMS related secret and private keys within a security module in accordance to the *CAMP Platform Security Document*.

Note: The SCMS provider may require a Level 3 conformant HSM.

3.3.5.10.4.2 Certificate Storage Security

The RSU shall store certificates that it owns, and all SCMS component certificates used as trust anchors within security modules in accordance with the *CAMP Platform Security Document*.

The RSU vendor may self-declare that it fulfills this requirement.

3.3.5.10.4.3 Secure Platform

The RSU shall fulfill the requirements for a secure platform as specified in the *CAMP Platform Security Document*.

3.3.5.10.5 Download CRL Requirements

This section contains requirements for an RSU to download certificate revocation list(s) (CRLs).

3.3.5.10.5.1 Download CRL Requirements - CAMP

The RSU shall download the CRLs for any SCMS participants that the RSU may communicate with in accordance with the CAMP's requirements in the *CAMP Platform Security Document.*

3.3.5.10.5.2 Download CRL Requirements – IEEE Std 1609.2.1

The RSU shall download the certificate revocation list(s) (CRL) for any SCMS participants that the RSU may communicate with in accordance with IEEE Std 1609.2.1™-2020.

3.3.5.10.5.3 Update CRL

The RSU shall at a minimum refresh its CRL at least once every two weeks.

3.3.5.10.6 Download SCMS Requirements

This section contains requirements for an RSU to download SCMS files.

3.3.5.10.6.1 Download SCMS Files - CAMP

The RSU shall download other SCMS files in accordance with the *CAMP Platform Security Document*.

3.3.5.10.6.2 Download SCMS Files – IEEE Std 1609.2.1

The RSU shall download other SCMS files in accordance with IEEE Std 1609.2.1™-2020.

3.3.5.10.6.3 Update SCMS Files

The RSU shall update other SCMS files in accordance with the *CAMP Platform Security Document* or IEEE Std 1609.2.1™-2020 requirements (as appropriate) at least once every two weeks.

3.3.5.11 Secure Administration Requirement

The RSU shall provide a secure administration user interface, network-accessible to the TMS.

3.3.5.12 Secure Management of Credentials Requirements

This section contains requirements for an RSU to securely manage its credentials.

3.3.5.12.1 Provision of Credentials

The RSU shall be placed into an initialization mode upon installation, whereby it is securely provisioned with credentials it uses to authenticate to external entities and credentials to trust.

3.3.5.12.2 Update Credentials

The RSU shall support a mechanism to securely update its provisioned credentials, including updating the status of the credentials to trust.

3.3.5.12.3 Expiration of Credentials

The RSU shall enable an operator to become aware of the upcoming expiration of certificates, within a configurable time window.

3.3.5.13 Logging for General and Security Purposes Requirement

The RSU shall be able to be configured to support the logging of security-relevant and general types of events. These are needed at least for diagnosis (e.g., of cyber attacks).

3.3.5.14 Secure Update Requirement

The RSU shall only install software/firmware updates that are verifiably trustworthy (e.g., signed by manufacturer).

Section 4
System Design Details [Normative]

Section 4 defines the system design details based on the requirements identified in the Functional Requirements section (see Section 3). Section 4 includes:

a) A tutorial
b) A Requirements Traceability Matrix (RTM). The RTM links the requirements presented in Section 3 with the design details that describe how to fulfill each requirement. Using this table, each requirement can then be traced in a conformant way.
c) Design Details. Contains the details, guidance and examples on how to fulfill a requirement.

Section 4 is intended for the following readers:

a) System integrators
b) Device manufacturers/vendors
c) Central system developers
d) Conformance testers
e) Other interested parties

For the first four categories of readers, Section 4 is useful in understanding how particular requirements are to be implemented and fulfilled. To conform to a functional requirement, the RSU shall implement all the details that trace to that requirement.

For the last category of readers, this section is useful to understand how particular functions and information are to be implemented to conform to the RSU Standard.

4.1 Tutorial [Informative]

The Requirements Traceability Matrix (RTM) in Section 4.2.3 identifies the standardized design details that fulfills each of the requirements defined in Section 3.3. The standardized design details that fulfill the requirements can be categorized as follows:

- Standardized design details that do not require additional explanation. Some requirements do not require additional details on how to fulfill the requirement - those requirements are identified by an N/A (Not Applicable) in the RTM.
- Standardized design details that require the exchange of data elements (called object definitions by NTCIP standards) to fulfill the requirement. The details of how the data elements are exchanged (called dialogs) are found in the normative reference that defines the data element.
- Standardized design details that require additional guidance or explanation. These design details are found in Section 4.3, Design Details.

4.2 Requirements Traceability Matrix

The Requirements Traceability Matrix (RTM) links the requirements as in Section 3.3 with the corresponding design details on the same line. Using this table, each requirement in Section 3.3 can thus be traced in a standardized way. Each requirement points to either other sections of the standard where the formal design details on how to fulfill the requirement is described, or points to data elements (object definitions) in a normative reference that fulfills the requirement. In the latter case, the formal definition of each data element and how the data element is to be exchanged is contained within the normative reference.

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 design details and data elements.

To conform to a requirement, an RSU system shall implement the design details traced from that requirement.

4.2.1 Notation [Informative]

4.2.1.1 Functional Requirement Columns

The functional requirements are defined within Section 3.3 and the RTM is based upon the requirements within that Section. The section number and the functional requirement name are indicated within these columns.

4.2.1.2 Design Details

The "Design Details" column either describes the standardized design details or references a section number where the standardized design details are defined within Section 4. A value of N/A indicates that no additional design information is necessary (i.e., the requirement is self-explanatory).

4.2.1.3 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.

4.2.2 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 are columns that define the standardized design details that fulfill the requirement. The columns either reference a section within this standard describing how the requirement is to be fulfilled; reference a normative reference, identification number and name of the data elements (object definitions) used to fulfill the functional requirement; or "No additional information provided" to indicate no additional design detail provided. The "Additional Specifications" column provides additional notes or details about the design content.

4.2.3 Requirements Traceability Matrix (RTM) Table

Table 12. Requirements Traceability Matrix (RTM)

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
3.3	Requirements		
3.3.1	General/Hardware/Mounting Requirements		
3.3.1.1	Power-over-Ethernet Plus (POE+)	See IEEE Std 802.3™-2018 Section Two, Clause 33. See Table 33-18 for the power supply limits, which includes the input voltage and other electrical parameters.	Component certification / listing
3.3.1.2	Environmental Requirements		
3.3.1.2.1	Ambient Temperature RSU	See NEMA TS 2-2016, Section 2.1.5.1, Ambient Temperature.	
3.3.1.2.2	Ambient Temperature Rate of Change RSU	See NEMA TS 2-2016, Section 2.1.5.1, Ambient Temperature.	
3.3.1.2.3	Storage Temperature RSU	See NEMA TS 2-2016, Section 2.1.5.1, Ambient Temperature.	
3.3.1.2.4	Humidity RSU	See NEMA TS 2-2016, Section 2.1.5.2, Humidity.	
3.3.1.2.5	Rain Resistance Test	See MIL-STD-810H Method 506.6 Rain, Procedure I.	
3.3.1.2.6	Corrosion Resistance Enclosure	See IEC 60529.	
3.3.1.2.7	Corrosion Resistance Test	See MIL-STD-810H Method 509.7 Salt Fog.	
3.3.1.3	Power Protection and Filtering Requirements		
3.3.1.3.1	Transients	See 4.3.1.1, Transients Design Details and IEC 61000-4-4:2012.	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
3.3.1.3.2	Surges	See IEC 61000-4-5:2017.	Note: This is a minimal requirement. Additional external surge protectors are recommended. For antenna wire greater than 10 feet to the antenna port, lightning protection for the antenna is recommended in certain areas.
3.3.1.4	Resistance to Shock and Vibration Requirements		
3.3.1.4.1	Vibration	See NEMA TS 2-2016, Section 2.2.3.	
3.3.1.4.2	Shock	See NEMA TS 2-2016, Section 2.2.4.	
3.3.1.4.3	Operational Vibration Test	See NEMA TS 2-2016, Section 2.2.8.	
3.3.1.4.4	Non-Operational Shock Test	See NEMA TS 2-2016, Section 2.2.9.	
3.3.1.5	Resistance to Electronic Emissions	See IEC 61000-6-2:2016.	
3.3.1.6	Out-of-Band and Out-of-Channel Interference Requirements		
3.3.1.6.1	IEEE Std 802.11 Out-of-Band and Out-of-Channel Interference Requirements	See IEEE Std 802.11™-2020 enhanced adjacent and non-adjacent channel rejection (dot11ACRType equal to 2).	
3.3.1.6.2	3GPP PC5 Mode 4 (Release 14 or 15) Out-of-Band and Out-of-Channel Interference Requirements	See 3GPP 36.521 (Release 14 or 15) for user equipment (UE).	
3.3.1.7	Resistant to Electrostatic Discharge	See 4.3.1.2, Resistant to Electrostatic Discharge Design Details.	
3.3.1.8	Limit Electronic Emissions Requirements		
3.3.1.8.1	Electronic Emissions	See CFR Title 47- Telecommunication: Chapter 1, Part 15 and Part 90.	
3.3.1.8.2	IEEE Std 802.11 Emissions Mask	See IEEE Std 802.11 STA transmit power class: Class C.	
3.3.1.8.3	3GPP PC5 Mode 4 (Release 14 or 15) Emissions Mask	See 3GPP 36.521 (Release 14 or 15).	
3.3.1.9	Mounting Requirements		

Requirements Traceability Matrix (RTM)

FR ID	Functional Requirement	Design Detail	Additional Specification
3.3.1.9.1	RSU Pole Mounting Requirements	No additional information provided.	Verify by inspection.
3.3.1.9.2	RSU Rack Mounting Requirements	No additional information provided.	Verify by inspection.
3.3.1.9.3	RSU Shelf Mounting Requirements	No additional information provided.	Verify by inspection.
3.3.1.9.4	RSU Wall Mounting Requirements	No additional information provided.	Verify by inspection.
3.3.1.10	Diagnostic Testing Requirements	Note: RSUs are expected to go through regression testing before being updated with new firmware/software/hardware.	
3.3.1.10.1	Diagnostic Setting – Forwarding Received Messages	See 4.3.1.3, Diagnostic Testing Design Details, and 4.3.1.3.1, Diagnostic Setting – Forwarding Received Messages Design Details.	
3.3.1.10.2	Diagnostic Setting - Forwarding Transmitted Messages	See 4.3.1.3, Diagnostic Testing Design Details, and 4.3.1.3.2, Diagnostic Setting – Forwarding Transmitted Messages Design Details.	
3.3.1.10.3	Diagnostic Setting - Storing Sent and Received Messages	See 4.3.1.3, Diagnostic Testing Design Details, and 4.3.1.3.3, Diagnostic Setting – Transmitting without Signature Design Details.	
3.3.1.10.4	Diagnostic Setting – Features Accessible through SNMP	No additional information provided.	
3.3.1.10.5	Diagnostic Setting – Transmitting without Signature	See 4.3.1.3, Diagnostic Testing Design Details.	
3.3.1.11	Maintainability Requirements		
3.3.1.11.1	Power Indication Requirements		
3.3.1.11.1.1	Power Indication	See 3.3.1.11.1.3, Power LED Characteristics	Verify by inspection.
3.3.1.11.1.2	Power Indication Location	See 4.3.1.4.1, Viewing Angle Design Details.	Verify by inspection.
3.3.1.11.1.3	Power LED Characteristics	See 4.3.1.4.1, Viewing Angle Design Details.	Verify by test.
3.3.1.11.2	Status Indication Requirements		
3.3.1.11.2.1	Status Indication	See 3.3.1.11.2.3, Status LED Characteristics	Verify by inspection.
3.3.1.11.2.2	Status Indication Location	See 4.3.1.4.1, Viewing Angle Design Details.	Verify by inspection.
3.3.1.11.2.3	Status LED Characteristics	See 4.3.1.4.1, Viewing Angle Design Details and 4.3.1.4.2, Status LED Characteristics Design Details.	Verify by test.
3.3.1.12	Quality Construction Requirements		
3.3.1.12.1	Edges	No additional information provided.	Verify by inspection.
3.3.1.12.2	Non-Electronic Hardware Materials	No additional information provided.	Verify by inspection or certification.

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
3.3.1.12.3	Electrical Isolation and Equipment Grounding	See TIA-607-D. Note: This requirement may be met by adding external surge protection device to the RSU's POE+ Ethernet connection.	Verify by inspection.
3.3.1.12.4	Electrical Installation and Integration	No additional information provided.	
3.3.1.12.5	Component Operational Requirements		
3.3.1.12.5.1	Maximum Ratings	No additional information provided.	Verify by inspection, certification or analysis.
3.3.1.12.5.2	PCB Locking Devices	No additional information provided.	Verify by inspection.
3.3.1.12.6	Manufacturer's Specifications	No additional information provided.	Verify by inspection of the design or manufacturer’s specification sheets.
3.3.1.12.7	Enclosure Surface Ultraviolet Protection (Discoloring)	No additional information provided.	Verify by test or self-declaration.
3.3.1.13	Interchangeability Requirements		
3.3.1.13.1	Ethernet Connector	No additional information provided.	Verify by inspection.
3.3.1.13.2	Powered Connector	No additional information provided.	Verify by inspection.
3.3.1.13.3	Antenna Connectors	See 4.3.1.5, Antenna Design Details.	Verify by inspection.
3.3.1.13.4	Open Standards	No additional information provided.	
3.3.1.13.5	Management Information Base	No additional information provided.	Provide and verify by inspection.
3.3.1.13.6	Communications Interface	No additional information provided.	Verify by inspection.
3.3.1.14	Software and Firmware Updates Requirements	See Annex A.3 of NTCIP 1218 v01 for design (dialogs and objects) corresponding to Functional Requirement IDs 3.5.1.1.5.1 to 3.5.1.1.5.3.	Note: Some firmware may not be updateable.
3.3.1.15	Size and Weight Requirements		
3.3.1.15.1	Weight	No additional information provided.	Verify by test.
3.3.1.15.2	Size	No additional information provided.	Verify by inspection.
3.3.1.16	User Safety Requirements	No additional information provided.	Verify by test.
3.3.2	Functional Requirements		
3.3.2.1	Startup Requirements		

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
3.3.2.1.1	RSU Startup Functions	See Annex A.3 of NTCIP 1218 v01 for design (dialogs and objects) corresponding to Functional Requirement IDs 3.5.1.1.4.1 to 3.5.1.1.4.5.	
3.3.2.1.2	RSU Restarts	No additional information provided.	
3.3.2.1.3	RSU Transition from Startup	See 4.3.2.1, RSU Transition from Startup Design Details.	
3.3.2.1.4	Application Configuration	See Annex A.3 of NTCIP 1218 v01 for design (dialogs and objects) corresponding to Functional Requirement IDs 3.5.1.4.2.1 and 3.5.1.4.2.2.	
3.3.2.2	Restart Requirements		
3.3.2.2.1	Remote Restart	See SET NTCIP 1218 v01: 5.17.4, rsuReboot to 1.	
3.3.2.2.2	Factory Settings	See 4.3.2.2, Factory Default Design Details.	Note: It may be desirable to keep the network interface settings.
3.3.2.2.3	Default Settings	No additional information provided.	
3.3.2.2.4	Log Restarts	See 4.3.2.3, Log Restarts Design Details.	
3.3.2.3	Time Keeping Requirements		
3.3.2.3.1	Track Time Requirements		
3.3.2.3.1.1	Time Reference	No additional information provided.	
3.3.2.3.1.2	Time Output	See ITU-R TF.460.6.	
3.3.2.3.1.3	Time Accuracy - Primary Time Source	No additional information provided.	Note: A PC5 system will likely have its own time source.
3.3.2.3.1.4	Leap Seconds	No additional information provided.	
3.3.2.3.2	Time Source Requirements		
3.3.2.3.2.1	Primary Time Source	No additional information provided.	
3.3.2.3.2.2	Report Primary Time Source	See Annex A.3 of NTCIP 1218 v01 for design (dialogs and objects) corresponding to Functional Requirement ID 3.5.2.3.1; and 4.3.2.4, Report Primary Time Source Design Details.	
3.3.2.3.2.3	Secondary Time Source	No additional information provided.	
3.3.2.3.2.5	Log Time Failures	See 4.3.2.5, Log Time Failures Design Details.	
3.3.2.3.2.6	Time Source Server	See 4.3.2.6, Time Source Server Design Details.	
3.3.2.4	Current Location Requirements		

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
3.3.2.4.1	Location Source	See GET NTCIP 1218 v01: 5.3.1, rsuGnssStatus.	
3.3.2.4.2	Report Location	See Annex A.3 of NTCIP 1218 v01 for design (dialogs and objects) corresponding to Functional Requirement IDs 3.5.2.4.1 and 3.5.2.4.5.	
3.3.2.4.3	Location Status	See GET NTCIP 1218 v01: 5.3.1, rsuGnssStatus.	
3.3.2.4.4	Log Location Failure – Satellites	See 4.3.2.7, Log Location Failure - Satellites Design Details.	
3.3.2.5	Network Interface Requirement	See Annex A.3 of NTCIP 1218 v01 for design (dialogs and objects) corresponding to Functional Requirement ID 3.5.1.2.1.2.	Note: Other interfaces, e.g., USB, may also be configured to operate as an IP network interface.
3.3.2.6	Performance and Data Requirements		
3.3.2.6.1	Operational Logging	See 4.3.2.8, Operational Logging Design Details.	
3.3.2.6.2	Statistical Data Requirements		
3.3.2.6.2.1	Log Interface Data	See 4.3.2.9, Log Interface Data Design Details.	
3.3.2.6.2.2	Log RF Communications Reception Coverage	See 4.3.2.10, Log RF Communications Reception Coverage Design Details.	
3.3.2.6.2.3	Report Number of Messages Exchanged by the V2X Radio	See 4.3.2.11, Report Number of Messages Exchanged by the V2X Radio Design Details.	
3.3.2.7	RSU Clustering Requirements		
3.3.2.7.1	RF Bandwidth Support Requirements - DSRC		
3.3.2.7.1.1	Configure Radio as a Service RSU	See 4.3.2.12, Configure Radio as a Service RSU Design Details.	
3.3.2.8	Message Handling Requirements		
3.3.2.8.1	Message Sent by the RSU Requirements		
3.3.2.8.1.1	Signing and Forwarding of Messages Not Signed by the Message Source	See 4.3.2.13.1, Signing and Forwarding of Messages Not Signed by the Message Source Design Details.	
3.3.2.8.1.2	Forwarding of Messages Signed by the Message Source	See 4.3.2.13.2, Forwarding of Messages Signed by the Message Source Design Details.	
3.3.2.8.1.3	Storing and Repeating Messages Not Signed by the Message Source	See 4.3.2.13.3, Storing and Repeating Messages Not Signed by the Message Source Design Details.	
3.3.2.8.1.4	Storing and Repeating Messages Signed by the Message Source	See 4.3.2.13.4, Storing and Repeating Messages Signed by the Message Source Design Details.	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
3.3.2.8.2	Forwarding of Messages Received by the RSU	See 4.3.2.13.5, Forwarding of Messages Received by the RSU Design Details.	
3.3.2.8.3	Message Transfer Latency		
3.3.2.8.3.1	Time Critical Messages	No additional information provided.	
3.3.2.8.3.2	Non-Time Critical Messages	No additional information provided.	
3.3.2.9	Application Requirements		
3.3.2.9.1	SPaT Processing Requirements		
3.3.2.9.1.1	NTCIP 1202	See 4.3.2.14.1, SPaT Processing Design Details and 4.3.2.14.2, SPaT Processing Design Details - NTCIP 1202.	
3.3.2.9.1.2	TSCBM	See 4.3.2.14.1, SPaT Processing Design Details and 4.3.2.14.3, SPaT Processing Design Details – TSCBM.	
3.3.2.9.2	BSM Processing Requirements		
3.3.2.9.2.1	BSM Filtering	See 4.3.2.14.4, BSM Filtering Design Details.	Note: NTCIP 1202 v03A 3.5.4.2.3.1 Configure Connected Device Detector Requirements define requirements to define zones and filter connected device data (e.g., BSMs and PSMs) based on the location of OBU/MU, its direction of travel and other criteria. See Annex A.3 of NTCIP 1202 v03A for 3.5.4.2.3.1.
3.3.3	Behavioral Requirements		
3.3.3.1	Configuration and Management Requirements		
3.3.3.1.1	Retrieve RSU Identity	See Annex A.3 of NTCIP 1218 v01 for design (dialogs and objects) corresponding to Functional Requirement IDs 3.5.1.1.1.1 to 3.5.1.1.1.5.	
3.3.3.1.2	Retrieve Configuration Version of the RSU	See Annex A.3 of NTCIP 1218 v01 for design (dialogs and objects) corresponding to Functional Requirement ID 3.5.1.1.2.	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
3.3.3.1.3	Configure RSU Location	See Annex A.3 of NTCIP 1218 v01 for design (dialogs and objects) corresponding to Functional Requirement IDs 3.5.1.1.3.1 to 3.5.1.1.3.5.	
3.3.3.1.4	Notifications	See Annex A.3 of NTCIP 1218 v01 for design (dialogs and objects) corresponding to Functional Requirement IDs 3.5.1.1.7.x.	Complete the PRL (Table 6) in NTCIP 1218 v01 for User Need ID 2.5.1.1.7 to determine which Notification requirements to support.
3.3.3.1.5	Configuration Error Resilience	See Annex G of NTCIP 1218 v01 for requirements on proper implementation of SNMP dialogs.	
3.3.3.1.6	Control Mode of Operation	See Annex A.3 of NTCIP 1218 v01 for design (dialogs and objects) corresponding to Functional Requirement ID 3.5.3.1.	
3.3.3.1.7	Control RF Antenna Output	See Annex A.3 of NTCIP 1218 v01 for design (dialogs and objects) corresponding to Functional Requirement ID 3.5.3.2.	Note: Caution - changing the power may result in a functional delay for the transmit power to take effect. Current LTE-V2X radio chips require a soft reboot of the radio chip.
3.3.3.1.8	Control Application	See Annex A.3 of NTCIP 1218 v01 for design (dialogs and objects) corresponding to Functional Requirement ID 3.5.3.4.	
3.3.3.2	Health and Status Monitoring Requirements		
3.3.3.2.1	Determine Mode of Operations	See Annex A.3 of NTCIP 1218 v01 for design (dialogs and objects) corresponding to Functional Requirement ID 3.5.2.2.	
3.3.3.2.2	Monitor Current Status	See 4.3.3.1, Monitor Current Status Design Details.	
3.3.3.2.3	Determine Operational Performance	See Annex A.3 of NTCIP 1218 v01 for design (dialogs and objects) corresponding to Functional Requirement IDs 3.5.2.1.1 to 3.5.2.1.8.	
3.3.3.2.4	Determine Operating Environment	See Annex A.3 of NTCIP 1218 v01 for design (dialogs and objects) corresponding to Functional Requirement IDs 3.5.2.10.1 and 3.5.2.10.2.	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
3.3.3.3	Visual Indications Requirements	See the Design Details for 3.3.1.11.	
3.3.4	Interface Requirements		
3.3.4.1	Back-Office Interface Requirement	See Annex A.3 of NTCIP 1218 v01 for design (dialogs and objects) corresponding to Functional Requirement IDs 3.5.1.2.1.1 to 3.5.1.2.1.3.	
3.3.4.2	V2X Interface Requirements		
3.3.4.2.1	Lower Layers and Radio Interfaces		
3.3.4.2.1.1	Transmit Power Requirements		
3.3.4.2.1.1.1	Transmit Power Range and Accuracy	No additional information provided.	
3.3.4.2.1.1.2	Transmit Power Monotonicity	No additional information provided.	
3.3.4.2.1.2	DSRC Requirements		
3.3.4.2.1.2.1	DSRC (IEEE Std 802.11)	See IEEE Std 802.11™-2020.	
3.3.4.2.1.2.2	Receiver Sensitivity (DSRC)	See IEEE Std 802.11™-2020.	
3.3.4.2.1.2.3	Multi-Channel Operations	See IEEE Std 1609.4™-2016.	
3.3.4.2.1.2.4	Maintain Channel Switching Operations	See 4.3.4.1, Maintain Channel Switching Operations Design Details.	
3.3.4.2.1.3	C-V2X Requirements		
3.3.4.2.1.3.1	C-V2X (3GPP PC5 Mode 4 (Release 14 or 15)) - Channel 183	See 3GPP PC5 Mode 4 (Release 14 or 15)	See SAE J3161 for guidance on configuring the PC5 interface.
3.3.4.2.1.3.2	C-V2X (3GPP PC5 Mode 4 (Release 14 or 15)) - Channel 180	See 3GPP PC5 Mode 4 (Release 14 or 15)	See SAE J3161 for guidance on configuring the PC5 interface.
3.3.4.2.1.3.3	Receiver Sensitivity (C-V2X)	See 3GPP PC5 Mode 4 (Release 14 or 15)	
3.3.4.2.2	Network and Transport Layer Requirements		
3.3.4.2.2.1	WAVE	See the PICS in Annex B.2 – IEEE Std 1609.3 PICS.	
3.3.4.2.2.2	WAVE Short Message Protocol	See the PICS in Annex B.2 – IEEE Std 1609.3 PICS.	
3.3.4.2.2.3	Internet Protocol	See the PICS in Annex B.2 – IEEE Std 1609.3 PICS.	
3.3.4.2.2.4	WAVE Service Advertisement	See the PICS in Annex B.3 – IEEE Std 1609.4 PICS; and Annex A.3 of NTCIP 1218 v01 for design (dialogs and objects) corresponding to Functional Requirement ID 3.5.1.3.3.2.	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
3.3.4.2.2.5	WAVE Router Advertisement	See the PICS in Annex B.3 – IEEE Std 1609.4 PICS; and Annex A.3 of NTCIP 1218 v01 for design (dialogs and objects) corresponding to Functional Requirement ID 3.5.1.3.3.2.4.	
3.3.5	Security Requirements		
3.3.5.1	V2X Interface Security Requirements		
3.3.5.1.1	V2X Interface Security - Sending Messages	See 4.3.5.1.1, Security - Sending V2X Messages Design Details.	
3.3.5.1.2	V2X Interface Security - Receiving and Forwarding Messages	See 4.3.5.1.2, Security - Receiving and Forwarding V2X Messages Design Details.	
3.3.5.2	Local and Back-Office Interface Security Requirements	See 4.3.5.2, Local and Back-Office Interface Security Design Details.	Note: While NTCIP 1218 v01 requires TLS v1.2, this standard is requiring an upgrade to TLS v1.3.
3.3.5.3	Manage Data Integrity Requirements		
3.3.5.3.1	Data Integrity - At Rest	See Annex A.3 of NTCIP 1218 v01 for the design (dialogs, objects) corresponding to Functional Requirement ID 3.6.1.2.1.	
3.3.5.3.2	Data Integrity - In Transit	See Annex A.3 of NTCIP 1218 v01 for 7. x. the design (dialogs, objects) corresponding to Functional Requirement ID 3.6.1.2.1.	
3.3.5.3.3	Device Integrity - Notification	See Annex A.3 of NTCIP 1218 v01 for 7. x. the design (dialogs, objects) corresponding to Functional Requirement IDs 3.5.1.1.7.3.1 and 3.5.1.1.7.3.2.	
3.3.5.4	Availability Requirements		
3.3.5.4.1	Manage Availability Requirements	See Annex A.3 of NTCIP 1218 v01 for 7. x. the design (dialogs, objects) corresponding to Functional Requirement IDs 3.5.4.2.1 and 3.5.4.2.2.	
3.3.5.4.2	Device Auditing Requirements	See Annex A.3 of NTCIP 1218 v01 for 7. x. the design (dialogs, objects) corresponding to Functional Requirement ID 3.5.1.1.7.3.5.	
3.3.5.5	Data Confidentiality Requirements	See Annex A.3 of NTCIP 1218 v01 for design (dialogs and objects) corresponding to Functional Requirement IDs 3.6.1.2.1 to 3.6.1.2.4.	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
3.3.5.6	Tamper Evident Requirements		
3.3.5.6.1	Tamper Evident Enclosure - Visual Requirements	See 4.3.5.6.1, Tamper Evident Enclosure - Visual Design Details.	
3.3.5.6.2	Tamper Evident Unused Port Requirements	See 4.3.5.6.2, Tamper Evident Port Design Details.	
3.3.5.6.3	Tamper Evident Enclosure - Bootup Requirements		
3.3.5.7	Private Key Storage Requirements	See 4.3.5.7, Certificate Storage Design Details.	
3.3.5.8	RSU Operating System Security Requirements		
3.3.5.8.1	RSU OS Applications and Services	See 4.3.5.8.1, RSU OS Applications and Services Design Details.	
3.3.5.8.2	RSU OS Ports and Protocols	See 4.3.5.8.2, RSU OS Ports and Protocols Design Details.	
3.3.5.8.3	RSU Password	See 4.3.5.8.3, RSU Password Design Details.	
3.3.5.9	Connection Assurance Requirements		
3.3.5.9.1	Assurance of Correct Connection Requirement	See 4.3.5.9.1, Assurance of Correct Initial Network Connection Design Details.	
3.3.5.9.2	Assurance of Continued Correct Connection Requirement	See 4.3.5.9.2, Assurance of Continued Correct Network Connection Design Details.	
3.3.5.10	SCMS Requirements		
3.3.5.10.1	SCMS Enrollment Requirements		
3.3.5.10.1.1	SCMS Enrollment Requirement - Bootstrapping	See 4.3.5.10.1.1, SCMS Bootstrap Design Details.	
3.3.5.10.1.2	SCMS Enrollment Requirement - CAMP	See 4.3.5.10.1.2, SCMS Enrollment Design Details - CAMP.	
3.3.5.10.1.3	SCMS Enrollment Requirement - IEEE Std 1609.2.1	See 4.3.5.10.1.3, SCMS Enrollment Design Details - IEEE Std 1609.2.1.	
3.3.5.10.2	SCMS Configurability Requirement	See 4.3.5.10.2, SCMS Configurability Design Details.	
3.3.5.10.3.1	SCMS Connectivity Requirement - CAMP	See 4.3.5.10.3.1, SCMS Connectivity Design Details - CAMP.	
3.3.5.10.3.2	SCMS Connectivity Requirement - IEEE Std 1609.2.1	See 4.3.5.10.3.2, SCMS Connectivity Design Details – IEEE Std 1609.2.1.	
3.3.5.10.4	Certificate and Private Key Storage Requirements		

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
3.3.5.10.4.1	Key Storage Security	See 4.3.5.10.4.1, Key Storage Security Design Details.	Note: The SCMS provider may require a Level 3 conformant HSM.
3.3.5.10.4.2	Certificate Storage Security	See 4.3.5.10.4.2, Certificate Storage Design Details.	
3.3.5.10.4.3	Secure Platform	See 4.3.5.10.4.3, Secure Platform Design Details.	
3.3.5.10.5	Download CRL Requirements		
3.3.5.10.5.1	Download CRL Requirements - CAMP	See 4.3.5.10.5.1, Download CRL Design Details - CAMP.	
3.3.5.10.5.2	Download CRL Requirements – IEEE Std 1609.2.1	See 4.3.5.10.5.2, Download CRL Design Details- IEEE Std 1609.2.1.	
3.3.5.10.5.3	Update CRL	See 4.3.5.10.5.3, Update CRL and SCMS Files Design Details.	
3.3.5.10.6.1	Download SCMS Files - CAMP	See 4.3.5.10.6.1, Download SCMS Files Design Details - CAMP.	
3.3.5.10.6.2	Download SCMS Files – IEEE Std 1609.2.1	See 4.3.5.10.6.2, Download SCMS Files Design Details- IEEE Std 1609.2.1.	
3.3.5.10.6.3	Update SCMS Files	See 4.3.5.10.5.3, Update CRL and SCMS Files Design Details.	
3.3.5.11	Secure Administration Requirement	See 4.3.5.11, Secure Administration Design Details.	
3.3.5.12	Secure Management of Credentials	See 4.3.5.12, Secure Management of X.509 Credentials for TLS Design Details.	
3.3.5.12.1	Provision of Credentials	See 4.3.5.12.1, Secure Interface for X.509 Credentials for TLS Design Details.	
3.3.5.12.2	Update Credentials	See 4.3.5.12.1, Secure Interface for X.509 Credentials for TLS Design Details.	
3.3.5.12.3	Expiration of Credentials	See 4.3.5.12.2, Notification – X.509 Credentials for TLS Signing Certificate Design Details; 4.3.5.12.3, Notification - X.509 Credentials for TLS Certificate Design Details; and 4.3.5.12.4, Expiration of Credentials Design Details.	
3.3.5.13	Logging for General and Security Purposes Requirement	See 4.3.2.8, Operational Logging Design Details, and 4.3.5.13, Logging for General and Security Purposes Design Details.	
3.3.5.14	Secure Update Requirement	See 4.3.5.14, Secure Update Design Details.	

4.3 Design Details

The specific design details to fulfill the requirements defined in Section 3.3 follow.

4.3.1 General / Hardware Design Details

The specific design details to fulfill the general/hardware requirements defined in Section 3.3.1 follow. All tests shall be conducted while the RSU is in operation.

4.3.1.1 Transients Design Details

The intent of requirement 3.3.1.3.1, Transients is that the RSU shall resume/restart normal operation after power interruptions of any duration, repetition rate, and duration of power available. The RSU must not be corrupted or fail to resume normal operation regardless of the power interruptions on the ethernet connection.

For testing purposes, it is recommended that the test RSU be subjected to power interruptions from 50 milliseconds to several seconds of power interruptions.

4.3.1.2 Resistant to Electrostatic Discharge Design Details

IEC 61000-4-2:2008 Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test Sections 7.1-7.2.2 in provides adequate design details to be able to successfully conduct electrostatic discharge testing. The physical properties for RSUs would enable the execution test design in accordance with Section 7.2.2 - Table-top equipment, further illustrated in Figure 4.

The following statement in IEC 61000-4-2:2008 meets the expected language for grounding the equipment during test "The EUT and ESD generator (including any external power supply) shall be grounded in accordance with their installation specifications. No additional rounding connections are allowed."

4.3.1.3 Diagnostic Testing Design Details

Diagnostic settings are used only for testing purposes; this mode is not for normal operations purposes and doing so can result in unsecure operations that can threaten both RSU and local and remote system operations. The specific design details to fulfill the requirements for diagnostic settings follow.

Guidance: It is recommended not to keep the RSU with these diagnostic settings enabled because production OBUs will not "use" the messages being broadcasted. Also, the RSU will be gray listed by the SCMS providers, and may not be able to get new certificates.

4.3.1.3.1 Diagnostic Setting – Forwarding Received Messages Design Details

This feature uses the design in 4.3.2.13.5, Forwarding of Messages Received by the RSU Design Details.

To properly implement this feature, the required entry shall be added to the rsuReceivedMsgTable. The NTCIP 1218 objects and their settings are shown in Table 13.

Table 13. Forwarding Received Message - Diagnostic Setting

NTCIP 1218 Object	Setting	Notes
rsuReceivedMsgIndex	Application specific	The PSID corresponding to the application associated with the message to be forwarded. Use 0xFFFFFFFF for all messages.
rsuReceivedMsgPsid	Application specific	Destination IP address of the message being forwarded
rsuReceivedMsgDestPort	Application specific	Destination port of the message being forwarded
rsuReceivedMsgProtocol	2	UDP
rsuReceivedMsgRssi	Deployment specific	Minimum received signal strength level for the message being forwarded
rsuReceivedMsgInterval	Deployment specific (1 - 10)	Interval of the message with the appropriate PSID to be forwarded
rsuReceivedMsgDeliveryStart	Deployment specific	Date and time the message should start being forwarded
rsuReceivedMsgDeliveryStop	Deployment specific	Date and time the message should stop being forwarded
rsuReceivedMsgSecure	Deployment specific	Indicates if security headers are to be forwarded
rsuReceivedMsgAuthMsgInterval	0	Disable authentication of message to be forwarded

4.3.1.3.2 Diagnostic Setting – Forwarding Transmitted Messages Design Details

The dialog associated with forwarding messages transmitted on the V2X interface for diagnostic purposes is shown in Figure 7. This feature uses an IP-based interface to send transmitted messages (to the V2X interface) to a remote system. NTCIP 1218 v01 objects are used to configure the feature.

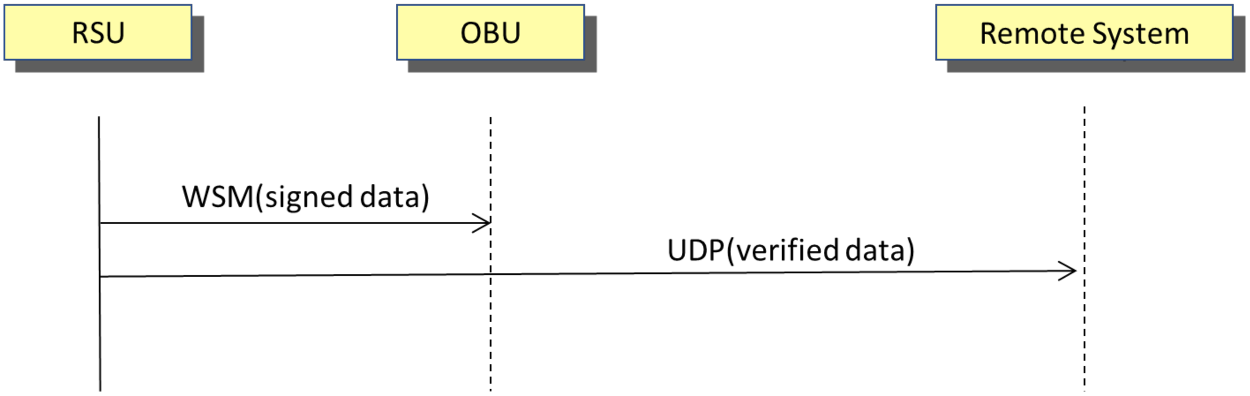


Figure 7. Dialog for Diagnostic Setting - Forwarding Transmitted Messages

The NTCIP 1218 v01 objects and their settings are shown in Table 14.

Table 14. Diagnostic Setting – Forwarding Transmitted Messages Design

NTCIP 1218 Object	Setting	Notes
rsuReceivedMsgIndex	Application specific	The PSID corresponding to the application associated with the message. Use 0xFFFFFFFF for all messages.
rsuReceivedMsgPsid	Application specific	Destination IP address of the message being forwarded
rsuXmitMsgFwdingDestPort	Application specific	Destination port of the message being forwarded
rsuXmitMsgFwdingProtocol	2	UDP
rsuXmitMsgFwdingDeliveryStart	Deployment specific	Date and time the message should start being transmitted
rsuXmitMsgFwdingDeliveryStop	Deployment specific	Date and time the message should stop being transmitted
rsuXmitMsgFwdingSecure	Deployment specific	Indicates if security headers are to be forwarded

4.3.1.3.3 Diagnostic Setting – Transmitting without Signature Design Details

The RSU shall have a diagnostic setting “diagnosticSigningDisabled” which disables signing messages which would otherwise be signed by the RSU based on other settings (e.g., rsuIFMOptions or rsuMsgRepeatOptions). When "diagnosticSigningDisabled" is set to "on", the RSU shall transmit all such WAVE messages with the IEEE Std 1609.2 header Ieee1609Dot2Data.unsecuredData. The default value for “diagnosticSigningDisabled” shall be “off”.

This shall affect any message configured and transmitted via the rsuMsgRepeatStatusTable with settings rsuMsgRepeatOptions.Bit0 = 1 (Process1609.2) and rsuMsgRepeatOptions.Bit1 = 0 (Secure). Similarly, this shall affect any message configured and transmitted via the rsuIFMStatusTable with settings rsuIFMOptions.Bit0 = 1 (Process1609.2) and rsuIFMOptions.Bit1 = 0 (Secure). Messages configured with other options, e.g., Bit0 = 0 (Bypass1609.2) are not affected.

This shall also affect any message created on the RSU itself when it is transmitted with a signature. For example, if a SPAT application on the RSU processes TSCBM from a controller and creates and transmits signed SPAT messages, then the RSU shall rather send these messages unsigned when “diagnosticSigningDisabled” is set to “on”.

If the message is signed elsewhere, the message will remain signed and still broadcasted.

It is recommended that an object be added to NTCIP 1218 v01 to support this requirement.

```
diagnosticSigningDisabled OBJECT-TYPE
   SYNTAX INTEGER { off (0), on (1) }
   MAX-ACCESS read-create
   STATUS current
   DESCRIPTION "<Definition> When this object is set to ON (1), the RSU
        transmits all 'signed' WAVE messages as 'unsigned' messages. Any WAVE
        message which would be signed by the RSU will be sent as an
        ‘unsigned’ message instead.  This setting overrides settings
        instructing the RSU to sign messages in other OIDs, for example
        rsuMsgRepeatOptions.secure (Bit 1) or rsuIFMOptions.secure (Bit 1).
        'Unsigned' messages are transmitted with the IEEE Std 1609.2 header
        Ieee1609Dot2Data.unsecuredData.
   <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.22"
   DEFVAL {0}
::= { rsuSysSettings 22 }
```

4.3.1.4 Maintainability Design Details

The specific design details to fulfill the functional requirements defined in Section 3.3.1.11 follow.

4.3.1.4.1 Viewing Angle Design Details

The viewing angle for the power and status indications on the RSU's enclosure shall be unobstructed by other objects, such as shutters. The viewing angle is twice the angle from the axis of the pixel to the 50% brightness point of the LED.

4.3.1.4.2 Status LED Characteristics Design Details

The colors in Table 10, Status LED Optical Characteristics can be produced by separate single color LEDs or a single tri-color LEDs where the color Amber is made by activating both the Red and Green anodes.

4.3.1.5 Antenna Design Details

For a rack-mounted, shelf-mounted or wall-mounted RSU, additional lightning suppression is recommended for the antenna cable.

Guidance: The procurement documents for the RSU site deployment should include appropriate lightning protection for the connections between the RSU and the field cabinet depending on the approach. This typically includes the ethernet connection and should include protection for the PoE insertion device(s). If external antennas are used, then the antenna connection should include appropriate lightning protection.

4.3.2 Functional Design Details

The specific design details to fulfill the functional requirements defined in Section 3.3.2 follow.

4.3.2.1 RSU Transition from Startup Design Details

NTCIP 1218 v01 defines an object, rsuModeStatus, describing the current mode of operation of the RSU. It is assumed that the RSU has the status of other (1) during the startup period, then will return the status any value other than other (1) after 120 seconds. The state machine definition for the other current mode of operations is found in NTCIP 1218 v01, Section 4.3.1, Operating Mode State Machine Definition.

4.3.2.2 Factory Default Design Details

The RSU factory default setting shall include the procedures necessary to transition the RSU back to the “manufacturing state”, per CAMP Platform Security Document.

Note: This procedure consists of a true wiping of the RSU, whereby all operational and SCMS identities, as well as all certificates are removed, and all cryptographic material in the HSM is zeroized. For the RSU to become operational again after this procedure, the processes of SCMS bootstrap, enrollment and initialization/configuration for non-SCMS use are necessary to be run again.

Note: NTCIP 1218 v01 does not support remotely reset a RSU to its factory default (See Annex E.24 Factory Default in NTCIP 1218 v01).

Note: It may be desirable to provide a flag to keep the network interface settings.

Guidance: the log files may not be available after a factory reset, so a user may wish to download the log files before setting to factory setting.

4.3.2.3 Log Restarts Design Details

The design for the system log and system log entries is defined in NTCIP 1218 v01 (See Annex A.3 of NTCIP 1218 v01 for 3.6.3.1). Table 15 represents the values for a system log entry for a RSU restart (reboot).

Table 15. Log Entry - Restarts

Object Name	Setting
PRI	NOTICE (or higher)
TIMESTAMP	The date and time when the RSU start
APP-NAME	Deployment specific
PROCID	Deployment specific
MSG	A reason for the reboot. At a minimum the RSU shall log as reasons: • "scheduled reboot": when it has been programmed to restart in regular intervals • "user reboot": when the user triggered a restart via NTCIP 1218 v01 (5.17.4) or other user interface • "comm loss reboot": when the RSU restarted due to communication loss as configured via NTCIP 1218 v01 (5.15.17) • "fault reboot": when the RSU detected a severe failure of a service or component and restarted in an attempt to fix the problem

4.3.2.4 Report Primary Time Source Design Details

See Annex A.3 of NTCIP 1218 v01 for design (dialogs and objects) corresponding to Functional Requirement ID 3.5.2.3.1, which describes the design details to fulfill this requirement.

Note: NTCIP 1218 v01: 5.17.5, rsuClockSource specifies the current primary time source for the RSU. The value for this object is expected to be gnss (3), consistent with requirement 3.3.2.3.2.1, Primary Time Source. If there are issues with GNSS time or the GNSS receiver, the value for rsuClockSource is expected to be ntp (4), consistent with requirement 3.3.2.3.2.3, Secondary Time Source.

4.3.2.5 Log Time Failures Design Details

A notification is transmitted, as defined in Annex A.3 of NTCIP 1218 v01 for 3.5.1.1.7.3.6, if no valid data is received from the primary time source. When the notification is transmitted, an entry also is written in the System Log with a priority of Critical as defined in Annex A.3 of NTCIP 1218 v01 for 3.6.3.4.

The Time Source Loss NOTIFICATION may be triggered by:

1. NTCIP 1218 v01: rsuClockSourceTimeout is an optional object definition specifying the allowable time, in seconds, that may elapse since valid data is received from the primary time source. A NOTIFICATION is triggered if the amount of time that has elapsed without valid data from the primary time source exceeds the value of NTCIP 1218 v01: 5.17.7 rsuClockSourceTimeout.
2. NTCIP 1218 v01: 5.17.8 rsuClockSourceFailedQuery is an optional data definition specifying the allowable number of consecutive failed query attempts for time information from the primary time source that is acceptable. A NOTIFICATION is triggered if the number of attempts to query the primary time source exceeds the value of NTCIP 1218 v01: 5.17. 8 rsuClockSourceFailedQuery.

The design for the system log and system log entries is defined in NTCIP 1218 v01 (See Annex A.3 of NTCIP 1218 v01 for 3.6.3.1). Table 16 represents the values for a system log entry for a Time Failure event.

Table 16. Log Entry - Time Failures

Object Name	Setting
PRI	NOTICE (or higher)

Object Name	Setting
TIMESTAMP	When the NOTIFICATION was generated
APP-NAME	Deployment specific
PROCID	Deployment specific
MSG	rsuTimeSourceLostMsg

Note: rsuTimeSourceLostMsg is a NTCIP 1218 v01 object (See NTCIP 1218 v01: 5.18.2.6) that contains the error message indicating a time source was lost.

4.3.2.6 Time Source Server Design Details

The design for the RSU to serve as an NTP server is defined by IETF RFC 5905 - Network Time Protocol Version 4: Protocol and Algorithms Specification.

4.3.2.7 Log Location Failure - Satellites Design Details

The design for the system log and system log entries is defined in NTCIP 1218 v01 (See Annex A.3 of NTCIP 1218 v01 for 3.6.3.1. The priority (PRI) for this entry is Critical and the number of satellites acquired is defined in NTCIP 1218 v01: 5.3.1, rsuGnssStatus.

4.3.2.8 Operational Logging Design Details

The design for the operational log is defined by NTCIP 1218 v01 which specifies the use of IETF RFC 5424, the Syslog Protocol for event messages. Requirements 3.6.3.x in Annex A.3 of NTCIP 1218 v01 describes the design details for using IETF RFC 5424 for NTCIP 1218 v01.

4.3.2.9 Log Interface Data Design Details

The design for log interface data is defined by NTCIP 1218 v01 which provides support to log all data transmitted to and received across an interface with the RSU. Requirements 3.5.1.2.3.x in Annex A.3 of NTCIP 1218 v01 describes the design for supporting logging the data transmitted and received.

NTCIP 1218 v01 provides a table, rsuInterfaceLogTable to configure what type of data should be logged in each log file. Each row defines the configuration of what data is to be logged, and maxRsuInterfaceLogs defines the maximum number of rows (configurations) in the table. rsuIfaceGenerate is a flag to enable or disable logging for each row (configuration), allowing different configurations to be stored and enabled as needed. The object, rsuIfaceName, defines which interface is logged (e.g., wlan0, gnss, dsrc). rsuIfaceLogStatus allows for the creation and deletion of rows (up to maxRsuInterfaceLogs).

The following objects are optional to be supported, as determined by the completed NTCIP 1218 v01 PRL (See Section 3.2.2.2):

- rsuIfaceLogByDir indicates what data across an interface is logged - data transmitted across the interface, data received across the interface, and all data across the interface (in a combined log file or separate log files)
- rsuIfaceStoragePath indicates the path (directory) where the log file can be found, and rsuIfaceLogName is the name of log file the logged data is stored in.
- rsuIfaceMaxFileSize specifies the maximum file size allowed
- rsuIfaceMaxFileTime specifies maximum number of hours of data that can be saved in a log file
- rsuIfaceLogOptions defines that the RSU should do if the disk is full and if the entries in the row (configuration) is deleted.
- rsuIfaceLogStart specifies the start time for logging the data
- rsuIfaceLogStop specifies the end time when the data logging should end

4.3.2.10 Log RF Communications Reception Coverage Design Details

NTCIP 1218 v01 supports the collection of statistics about the effective RF communications range (receiver only) around the RSU. Using information in the validated messages received by the RSU from the V2X radio(s), the RSU stores the farthest distance and the average farthest distance from the RSU that a validated message was received over a time period. Requirements 3.5.2.8.x in Annex A.3 of NTCIP 1218 v01 describes the design for supporting the collection of these statistics.

NTCIP 1218 v01 provides a table, rsuCommRangeTable to configure and store the collection of this data. Each row defines the configuration of what data is to be collected, and maxRsuCommRange defines the maximum number of rows (configurations) in the table. rsuCommRangeSector defines which sector to collect data for - each sector represents a 22.5 degree slice of area around the RSU, starting from the North direction. rsuCommRangeMsgId defines which SAE J2735 message to collect data for (including any SAE J2735 message), while rsuCommRangeFilterType and rsuCommRangeFilterValue allows the data to be filtered by vehicle type (SAE J2735: DE_VehicleType) or vehicle class (SAE J2735: DE_BasicVehicleClass).

Data is then stored in each of six "bins": 3 for the farthest distance and 3 for the average farthest distance; for over 1-, 5-, and 15- minute periods. Each bin is a rolling period, where the 1 minute bin is up to 59 seconds old, and 5- and 15- minute bins would then be the farthest or average farthest distance over the past 5- (or 15-) 1-minute bins. rsuCommRangeStatus allows for the creation and deletion of rows (up to maxRsuCommRange).

4.3.2.11 Report Number of Messages Exchanged by the V2X Radio Design Details

The design for the report that describes the number of messages exchanged by the V2X radio is defined by NTCIP 1218 v01 which supports the collection of statistical data on the number of messages transmitted and received by the RSU. Requirement 3.5.2.6 in Annex A.3 of NTCIP 1218 v01 describes the design for supporting the collection of these statistics.

NTCIP 1218 v01 provides a table, rsuMessageCountsByPsidTable, to configure and store the collection of this data. Each row defines the configuration of what data is to be collected, and maxRsuMessageCountsByPsid defines the maximum number of rows (configurations) in the table. rsuMessageCountsByPsidId defines which Provider Service Identifier (PSID) to collect data for, rsuMessageCountsByChannel defines which V2X channel to collect data for, and rsuMessageCountsDirection defines which direction (inbound, outbound or both directions) to collect data for. rsuMessageCountsByPsidTime can be used by the RSU to indicate when it started the message count, or it can be configured to indicate the time the message counter should begin by setting a date and time in the future. The date and time are an octet string of 8 octets as defined in SNMPv2-TC, consisting of year (2 octets), month, day, hour, minutes, seconds, and deci-seconds.

rsuMessageCountsByPsidCounts is the counter and represents the number of messages that were exchanged since the start time and satisfies the criteria in that row. rsuMessageCountsByPsidRowStatus allows for the creation and deletion of rows (up to maxRsuMessageCountsByPsid).

4.3.2.12 Configure Radio as a Service RSU Design Details

This section describes the design details to configure one radio as a service RSU. A "service RSU" is defined as an RSU offering a particular service identified by a PSID on a specific DSRC channel without advertising the service via WSAs. The WSA informing OBUs about the available service on this DSRC channel is rather broadcast by a nearby "primary RSU". The primary / service radio pairing allows the service RSU’s radios to be tuned to channels used for services only and don’t need to switch to the control channel (178) for WSA broadcasts.

A service RSU has its radios configured via the corresponding NTCIP 1218 OIDs for radio configuration. Applicable OIDs for this configuration are specified in NTCIP 1218 v01: 5.2.2 Radio Table (rsuRadioTable).

The primary RSU broadcasts the WSAs for those services. Applicable OIDs for the WSA configuration are specified in NTCIP 1218 v01: 5.10.2 WAVE Service Advertisement Service Table (rsuWsaServiceTable) and NTCIP 1218 v01: 5.10.3 WAVE Service Advertisement Channel Table (rsuWsaChannelTable).

4.3.2.13 Message Handling Design Details

This section provides the functional design associated with message handling. Messages are transmitted or received and forwarded according to this design. Messages are payloads received via the IEEE Std 1609.3™-2020 WAVE Short Message Protocol (WSMP). Local systems include the RSCE, and remote systems include the TMS and back office system.

4.3.2.13.1 Signing and Forwarding of Messages Not Signed by the Message Source Design Details

The dialog associated with signing and forwarding operations is shown in Figure 8. This feature uses an SNMP set operation along with NTCIP 1218 v01 objects used to configure the feature.

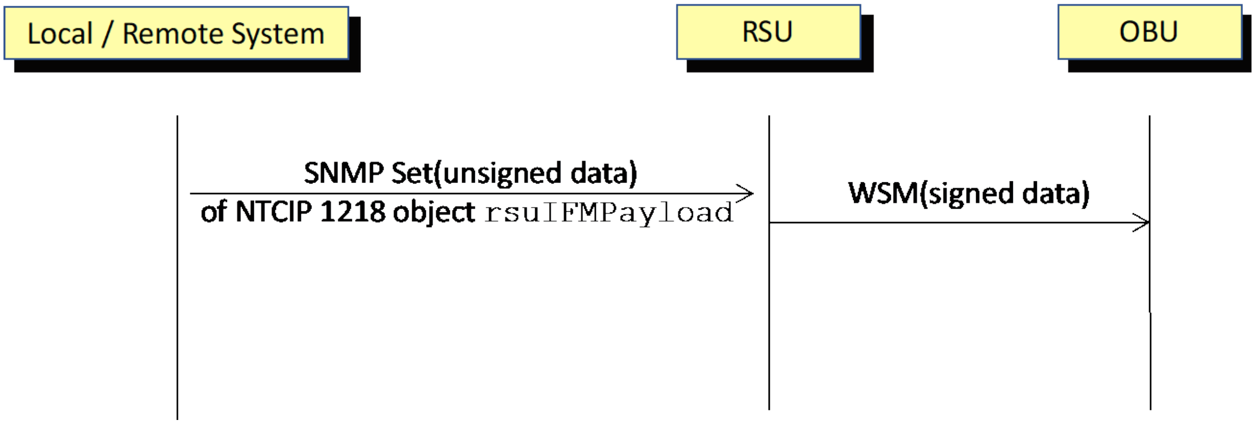


Figure 8. Dialog for Signing and Forwarding of Messages Not Signed by the Message Source

The NTCIP 1218 v01 objects and their settings are shown in Table 17.

Table 17. Signing and Forwarding of Messages Not Signed Design

NTCIP 1218 Object	Setting	Notes
rsuIFMPsid	Application specific	The PSID corresponding to the application associated with the message and its corresponding security profile
rsuIFMTxChannel	Deployment specific	The transmission RF channel
rsuIFMEnable	1	Set to 1 to enable forwarding
rsuIFMPriority	Application specific	The priority of the message (0 through 7)
rsuIFMOptions	Bit 0 = 1 Bit 1 = 0 Bit 2 = 0 (default) Bit 3 = 0 (default)	RSU shall sign message per IEEE Std 1609.2™ before forwarding, message as received from source is not secure
rsuIFMPayload	Payload	The contents of the message

4.3.2.13.2 Forwarding of Messages Signed by the Message Source Design Details

The dialog associated with forwarding operations for already signed messages is shown in Figure 9. This feature uses an SNMP set operation along with NTCIP 1218 v01 objects to configure the feature.

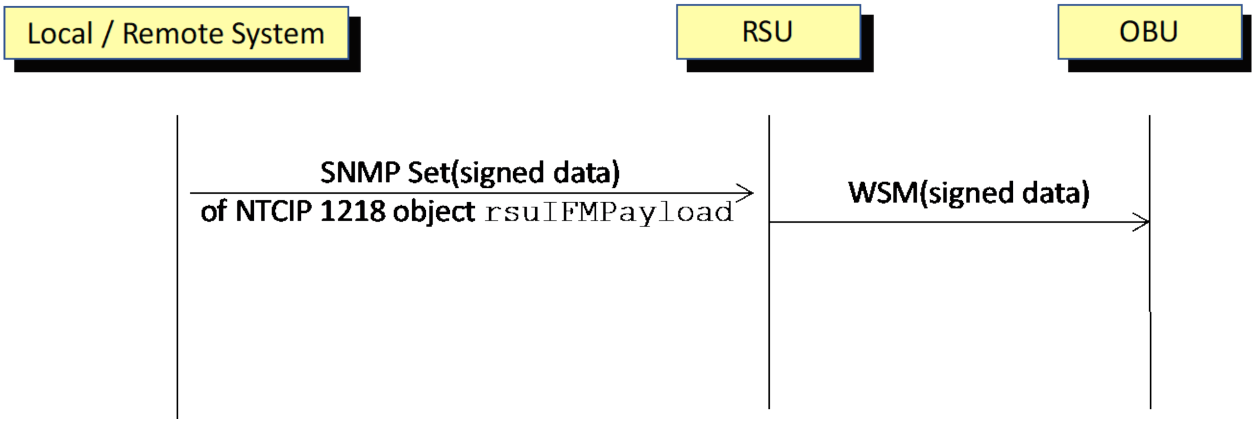


Figure 9. Dialog for Forwarding of Messages Signed by the Message Source

The NTCIP 1218 objects and their settings are shown in Table 18.

Table 18. Forwarding of Messages Signed Design

NTCIP 1218 Object	Setting	Notes
rsuIFMPsid	Application specific	The PSID corresponding to the application associated with the message and its corresponding security profile
rsuIFMTxChannel	Deployment specific	The transmission RF channel
rsuIFMEnable	1	Set to 1 to enable forwarding
rsuIFMPriority	Application specific	The priority of the message (0 through 7)
rsuIFMOptions	Bit 0 = 0 Bit 1 = 0 Bit 2 = 0 (default) Bit 3 = 0 (default)	RSU does not sign message before forwarding, message as received from source is secure
rsuIFMPayload	Payload	The contents of the message

4.3.2.13.3 Storing and Repeating Messages Not Signed by the Message Source Design Details

The dialog associated with storing and repeating operations for unsigned messages is shown in Figure 10. This feature uses an SNMP set operation along with NTCIP 1218 v01 objects to configure the feature. The message is signed and certificate attached according to the IEEE Std 1609.2™-2016 security profile for the corresponding PSID prior to storing.

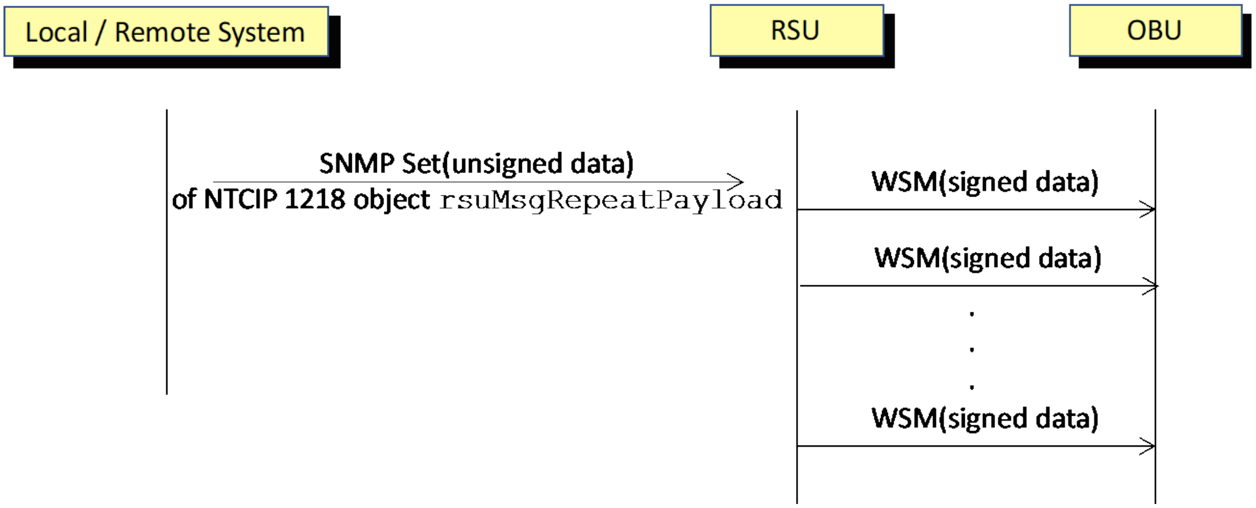


Figure 10. Dialog for Storing and Repeating of Messages Not Signed by the Message Source

The NTCIP 1218 v01 objects and their settings are shown in Table 19.

Table 19. Storing and Repeating Messages Not Signed Design

NTCIP 1218 Object	Setting	Notes
rsuMsgRepeatPsid	Application specific	The PSID corresponding to the application associated with the message
rsuMsgRepeatTxChannel	Deployment specific	The transmission RF channel
rsuMsgRepeatTxInterval	Application specific	Time between message transmissions
rsuMsgRepeatDeliveryStart	Deployment specific	Date and time the message should start being transmitted
rsuMsgRepeatDeliveryStop	Deployment specific	Date and time the message should stop being transmitted
rsuMsgRepeatPayload	Payload	The contents of the message
rsuMsgRepeatEnable	1	Set to 1 to enable
rsuMsgRepeatPriority	Application specific	The priority of the message (0 through 7)
rsuMsgRepeatOptions	Bit 0 = 1 Bit 1 = 0 Bit 2 = 0 (default) Bit 3 = 0 (default)	RSU shall sign message per IEEE Std 1609.2™ before forwarding, message as received from source is not secure

4.3.2.13.4 Storing and Repeating Messages Signed by the Message Source Design Details

The dialog associated with storing and repeating operations for signed messages is shown in Figure 11. This feature uses an SNMP set operation along with NTCIP 1218 v01 objects to configure the feature.

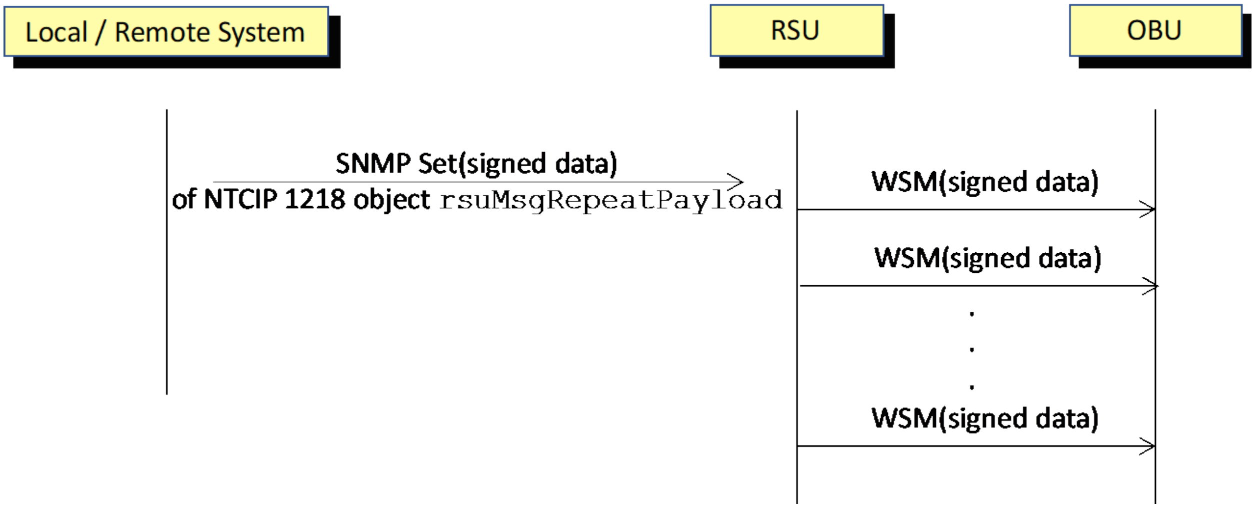


Figure 11. Dialog for Storing and Repeating of Messages Already Signed by the Message Source

The NTCIP 1218 v01 objects and their settings are shown in Table 20.

Table 20. Storing and Repeating of Messages Already Signed Design

NTCIP 1218 Object	Setting	Notes
rsuMsgRepeatPsid	Application specific	The PSID corresponding to the application associated with the message
rsuMsgRepeatTxChannel	Deployment specific	The transmission RF channel
rsuMsgRepeatTxInterval	Application specific	Time between message transmissions
rsuMsgRepeatDeliveryStart	Deployment specific	Date and time the message should start being transmitted
rsuMsgRepeatDeliveryStop	Deployment specific	Date and time the message should stop being transmitted
rsuMsgRepeatPayload	Payload	The contents of the message
rsuMsgRepeatEnable	1	Set to 1 to enable
rsuMsgRepeatPriority	Application specific	The priority of the message (0 through 7)
rsuMsgRepeatOptions	Bit 0 = 0 Bit 1 = 0 Bit 2 = 0 (default) Bit 3 = 0 (default)	RSU does not sign message before storing and repeating, since message as received from source is secure

4.3.2.13.5 Forwarding of Messages Received by the RSU Design Details

The dialog associated with forwarding messages received on the V2X interface is shown in Figure 12. This feature uses an IP-based interface to send received messages to the local or remote system, only after verifying the signature of the message payload. NTCIP 1218 v01 objects are used to configure the feature.

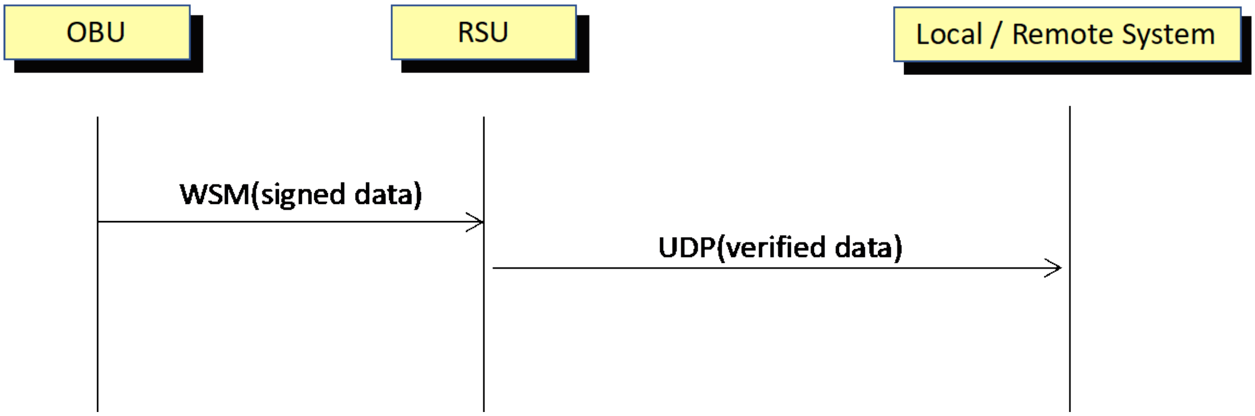


Figure 12. Dialog for Forwarding of Messages Received by the RSU

The NTCIP 1218 v01 objects and their settings are shown in Table 21.

Table 21. Forwarding of Messages Received Design

NTCIP 1218 Object	Setting	Notes
rsuReceivedMsgPsid	Application specific	The PSID corresponding to the application associated with the message
rsuReceivedMsgDestIpAddr	Application specific	Destination IP address of the message being forwarded
rsuReceivedMsgDestPort	Application specific	Destination port of the message being forwarded
rsuReceivedMsgProtocol	2	UDP
rsuReceivedMsgRssi	Application specific	The minimum received signal strength threshold for a received message to be forwarded
rsuReceivedMsgInterval	1	Every message is forwarded
rsuReceivedMsgDeliveryStart	Deployment specific	Date and time the message should start being transmitted
rsuReceivedMsgDeliveryStop	Deployment specific	Date and time the message should stop being transmitted
rsuReceivedMsgSecure	0	Security headers are not forwarded
rsuReceivedMsgAuthMsgInterval	1	For every received message, before forwarding, signed SPDU is verified per IEEE Std 1609.2™ and the PSID-specific security profile, including checking SSP against message payload if appropriate

Guidance: Check with the RSU vendor on the processing capacity of the RSU to process BSMs.

4.3.2.14 Application Design Details

This section describes the design details for applications.

4.3.2.14.1 SPaT Processing Design Details

The dialog associated with transmitting SPaT messages using SPaT information received from the RSCE is shown in Figure 13. This feature uses interfaces defined in NTCIP 1202 v03A or TSCBM to send SPaT information from the RSCE/traffic signal controller to the RSU. The RSU receives the SPaT information, then formats it into a SAE J2735_202007 SPaT message with UPER encoding, signs the message according to the IEEE Std 1609.2™-2016 security profile associated with PSID 0x82 (0p80-02), and transmits it using the IEEE Std 1609.3™-2020 WAVE Short Message Protocol (WSMP). The RSU's SPaT processing may include filling in values for data elements required in the SAE J2735_202007 SPaT message, such as the DE_IntersectionStatus object.

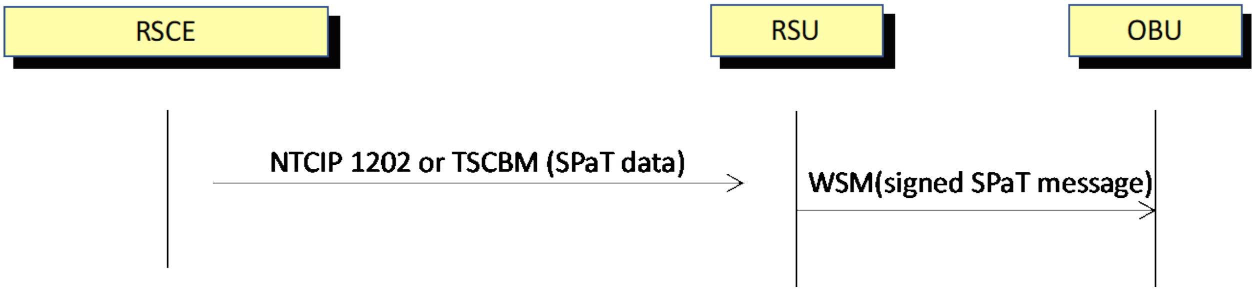


Figure 13. Dialog for SPaT Processing

4.3.2.14.2 SPaT Processing Design Details - NTCIP 1202

NTCIP 1202 Interface
The RSU shall implement the SNMP agent role as defined in NTCIP 1202 v03A, Annex F.3.3.3. To do so the RSU may provide its own SNMP agent IP port or integrate with the main RSU SNMP agent which also implements NTCIP 1218 v01.

At a minimum the RSU shall implement the following NTCIP 1202 v03A OIDs:

- spatStatus (7.2.1)
- signalStatusBlock (7.2.8)
- movementManeuverStatusBlock (7.2.9)

The SNMP agent port shall be secured using the same protocols and measures defined in the Security Design Details section (Section 4.3.5) of this standard.

Assumption: This design is based on a 1:1 mapping between a SPaT message from a traffic signal controller and a MAP message. Situations beyond this assumption, such as a RSU supporting multiple traffic signal controllers is not addressed in this standard but is allowed.

NTCIP 1202 Message Processing
The RSU shall construct a valid SPaT based on:

- IntersectionReferenceID (obtained from the MAP message configured in the Store and Repeat Message table (rsuMsgRepeatStatusTable))
- Processing the spatStatus content and mapping it one-to-one to corresponding content of the SPaT’s IntersectionStatusObject.
- Processing the channelSignalData within received signalStatusBlocks and mapping it to corresponding content to the SPaT’s MovementState for each SignalGroupID referenced by the configured MAP message.
  Note: The channel numbers within the signalStatusBlock do not necessarily correspond one-to-one to SignalGroupIDs within the SPaT message and may require additional mapping configuration.
- Processing the movementManeuverStatusData within received movementManeuverStatusBlocks and mapping it to corresponding content to the SPaT’s ConnectionManeuverAssist for each LaneConnectionID referenced by the configured MAP message. Further the content of movementManeuverState informs the mapping of the SPaT’s MovementState for each SignalGroupID.
  Note: The main content of each movementManeuverStatusData block is indexed by channel

number plus movementManeuverIndex. This compound index does not correspond one-to-one to LaneConnectionIDs within the SPaT message and will require additional mapping configuration.

- The RSU shall set the "noValidSPATisAvailableAtThisTime" Bit in the IntersectionStatusObject on the SAE J2735 SPAT message" for ANY error discovered related to the NTCIP 1202 input, including If no NTCIP 1202 data has been received within the last 200 milliseconds.

The RSU shall process the Actuated Signal Controller's (ASC) tick count information as follows:

- The signalStatusBlock contains the ascCurrentTick (5.17.6) value in the first 2 bytes of the block.
- The RSU shall process ascCurrentTick values as a heartbeat from the ASC. If no ascCurrentTick has been received within the last 200 milliseconds, the RSU shall set the “noValidSPATisAvailableAtThisTime” Bit in the IntersectionStatusObject of the SPaT message.
- The RSU shall record the time when an ascCurrentTick was received as rsuCurrentTickReceivedTime based on the RSU’s GNSS time source.
- The RSU shall convert the tick counts received from the ASC to SPaT TimeMark values as follows:
    - Calculate remaining deciseconds for a channel’s signalState as follows:
      remainingMinEnd ::= signalStateMinEndTick - ascCurrentTick
      remainingMaxEnd ::= signalStateMaxEndTick - ascCurrentTick
      remainingLikelyEnd ::= signalStateLikelyEndTick - ascCurrentTick (if signalStateLikelyEndTime is provided by the ASC)
    - Calculate the TimeMark value to put into the constructed SPaT as follows:
      minEndTime ::= remainingMinEnd + rsuCurrentTickReceivedTime
      maxEndTime ::= remainingMaxEnd + rsuCurrentTickReceivedTime
      likelyTime ::= remainingLikelyEnd + rsuCurrentTickReceivedTime (if remainingLikelyEndTime is provided by the ASC)

More detailed specification of the RSU’s SPaT processing is outside the scope of this standard.

4.3.2.14.3 SPaT Processing Design Details – TSCBM

TSCBM Interface
The RSU shall listen on a configurable UDP port for TSCBM messages. The RSU shall receive Traffic Signal Controller Broadcast Message (TSCBM) from a compatible ASC per NTCIP 1202 v03A Section E.1.10 and per NEMA TS 10-2020, Section 5.5.1.

Note: This UDP-based communication is not secured and the received message cannot be authenticated when implemented this way. However, TSCBM has been implemented this way by most controller software vendors.

Assumption: This design is based on a 1:1 mapping between a SPaT message from a traffic signal controller and a MAP message. Situations beyond this assumption, such as a RSU supporting multiple traffic signal controllers is not addressed in this standard but is allowed.

TSCBM Message Processing
The RSU shall construct a valid SPaT based on:

- IntersectionReferenceID (obtained from the MAP message configured in the Store and Repeat Message table (rsuMsgRepeatStatusTable))
- Processing the information contained in the TSCBM:
    - SPaT IntersectionStatusObject shall be populated from byte 232 / spatIntersectionStatus
    - SPaT MovementState for each SignalGroupID referenced by the configured MAP message shall be populated from the information contained in bytes 2 – 231 of the TSCBM.

- The RSU shall monitor the reception of TSCBM in regular intervals. If no TSCBM has been received within the last 200 milliseconds, the RSU shall set the “noValidSPATisAvailableAtThisTime” Bit in the IntersectionStatusObject of the SAE J2735 SPAT message.
- RSU shall set the "noValidSPATisAvailableAtThisTime" Bit in the IntersectionStatusObject on the SAE J2735 SPAT message" for ANY error discovered related to the TSCBM input.

The RSU shall sign the SPaT per IEEE Std 1609.2™-2016 and the SPaT security profile, which can be found in the Connected Intersections (CI) Implementation Guide, Annex C.1, Security Profile for SPaT Messages.

More detailed specification of the RSU’s SPaT processing is outside the scope of this standard.

4.3.2.14.4 BSM Filtering Design Details

The RSU shall support the configuration of geographical zones for the purpose of detecting that a vehicle entered a zone based on the vehicle’s location contained within the received BSMs. At a minimum the RSU shall support a rectangular zone where the rectangle is defined by 2 points A and B plus a width (See Figure 14).

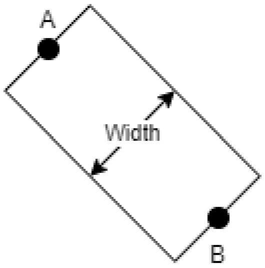


Figure 14. BSM Filtering Zone

Additional zone properties like elevation and heading as well as additional zone types may be supported by the RSU.

The RSU shall identify each zone by an ID of type INTEGER and a name of type (DisplayString).

The RSU shall support at a minimum the event type “ZoneEnter”. The ZoneEnter event is triggered when a BSM is received with BSM.coreData.lat and BSM.coreData.long identifying a coordinate within the zone for a vehicle identified by BSM.coreData.id for the first time. Subsequently, received BSMs from that same vehicle identified by BSM.coreData.id with coordinates within the zone shall only trigger the ZoneEnter event again when the vehicle has left the zone. Additional criteria such as vehicle heading and elevation may be used by the RSU to determine ZoneEnter depending on the RSU’s capabilities.

The RSU may support the event type “ZoneExit”. The ZoneExit event is triggered when a BSM is received with BSM.coreData.lat and BSM.coreData.long identifying a coordinate outside the zone for a vehicle identified by BSM.coreData.id which previously triggered a ZoneEnter event.

The RSU shall support time-based and location-based hysteresis in order to suppress repeated ZoneEnter (and ZoneExit) events which are caused by location inaccuracy. For time-based hysteresis the RSU shall support a configurable `minimumExitTime`. A tracked vehicle shall only be considered to have left the zone (ZoneExit event), if BSMs with locations outside the zone have been received for at least `minimumExitTime`. Note: This time threshold is different from the time threshold for no longer receiving any BSMs from the vehicle and considering it gone for that reason.

For location-based hysteresis the RSU shall support a configurable `minimumExitDistance`. A tracked vehicle shall only be considered to have left the zone (ZoneExit event), if BSMs with locations outside the zone have been received with a distance between the perimeter of the zone and the vehicle of at least `minimumExitDistance`.

Note: Both the time-based hysteresis and the location-based hysteresis are evaluated simultaneously. Therefore, a vehicle shall be considered to have left the zone if it either has left the zone for at least `minimumExitTime` or if it has moved outside the zone for at least `minimumExitDistance`, whichever occurs first.

The RSU shall support subscription of a client application to zone events such as “ZoneEnter” via the ZoneEventTable.

```
rsuZoneEventTable OBJECT-TYPE
    SYNTAX SEQUENCE OF rsuZoneEventEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Contains the subscriptions to zone events
      being sent to a network host, the IP Address and port number of the
      destination host, as well as other configuration parameters as defined.
    <TableType>  static
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.21.2"
::= { rsuZoneEvent 2 }

rsuZoneEventEntry OBJECT-TYPE
    SYNTAX       RsuZoneEventEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> A row describing the RSU Zone Event Entry.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.21.2.1"
    INDEX        { rsuZoneEventSubscrIndex }
::= { rsuZoneEventTable 1 }

RsuZoneEventEntry ::= SEQUENCE {
    rsuZoneEventSubscrIndex             RsuTableIndex,
    rsuZoneEventSubscrZoneID            Integer32,
    rsuZoneEventSubscrEventType         DisplayString,
    rsuZoneEventSubscrDestIpAddr        DisplayString,
    rsuZoneEventSubscrDestPort          Integer32,
    rsuZoneEventSubscrProtocol          INTEGER,
    rsuZoneEventSubscrSecure            INTEGER,
    rsuZoneEventSubscrStatus            RowStatus     }
```

For protocol “udp (2)” the RSU shall send the following structure in COER format to subscribers:

```
RsuZoneEventMsg ::= SEQUENCE {
    version                             INTEGER { v1(1) },
    rsuZoneEventSubscrZoneID            INTEGER (1..16),
    rsuZoneEventSubscrEventType         DisplayString,
    rssi                                Integer32 (-100..-60),
    signature                           INTEGER { unsigned(0), signed(1) },
    rsuZoneEventSubscrMsgPayload        OCTET STRING (SIZE(1..2302)) }
```

The rsuZoneEventSubscrMsgPayload shall contain the BSM which triggered the event. The content of this field further depends on the setting of rsuZoneEventSubscrSecure which is defined as:

```
A value of 0 indicates the RSU is to forward the entire WSMP
payload, including certificates and signature. A value of 1
indicates the RSU is to forward only that payload inside the
Ieee1609Dot2Data frame in UPER format. So either
Ieee1609Dot2Data.unsecuredData or
Ieee1609Dot2Data.signedData.tbsData.payload.data.unsecuredData.
```

See Annex C.3.6, Support for BSM Filtering, for the complete object definitions.

4.3.3 Behavioral Design Details

The specific design details to fulfill the behavioral requirements defined in Section 3.3.3 follow.

4.3.3.1 Monitor Current Status Design Details

There are several object definitions in NTCIP 1218 v01 that collectively provides a comprehensive picture of the RSU's status. Table 22 lists those object definitions and the expected values for those objects. Any other value for an object may indicate a potential issue with the RSU. See Annex A.3 in NTCIP 1218 v01 for each requirement to determine the appropriate dialog (sequence of data exchanges) to GET the value for each object.

Table 22. Current Operational Status

NTCIP 1218 Object	Expected Value	Notes
rsuSecEnrollCertStatus	enrolled (4)	
rsuSecAppCertState	valid (2)	For each application PSID.
rsuChanStatus	NOT nonOp (3)	Note: For DSRC Only. • bothOp (0) indicates both continuous and alternating mode are operational • altOp (1) indicates alternating mode is operational but continuous mode is not operational • contOp (2) indicates continuous mode is operational but alternating mode is not operational
rsuModeStatus	operate (2) or standby (3)	As desired
rsuClockSource	gnss (3)	
rsuClockSourceStatus	active (2)	
rsuStatus	okay (2)	
rsuServiceStatus	okay (2)	For each RSU service.

4.3.4 Interface Design Details

The specific design details to fulfill the interface requirements defined in Section 3.3.4 follow.

4.3.4.1 Maintain Channel Switching Operations Design Details

The purpose of the requirement is for the RSU to maintain a limited but feasible level of operation in the event of prolonged outage of the primary time source. The primary time source is required for maintaining alternating channel operation as well as accurate time stamping of safety-critical messages like SPAT.

For example, broadcast of the MAP message is still possible as it is sent on channel 172 in continuous mode and doesn't require highly accurate timestamps. It is also useful because OBUs then know that the intersection is equipped but (apparently) unable to send proper SPAT.

After the minimum one-minute period following no valid data being available from the primary time source, the following message types may still be transmitted:

- WAVE Service Advertisement (WSA) messages
- MAP messages
- All Immediate Forward messages that are already signed by the source
- All Store and Repeat messages that are already signed by the source

4.3.5 Security Design Details

This section contains the design details to fulfill the security requirements defined in Section 3.3.5.

4.3.5.1 V2X Interface Security Design Details

This section contains the security design details for the V2X interface.

4.3.5.1.1 Security - Sending V2X Messages Design Details

The RSU shall verify or apply IEEE Std 1609.2™-2016 signatures to all messages it sends over the V2X interface unless the RSU has a diagnostic setting enabled (See Section 4.3.1.3).

The RSU shall fulfill the requirements specified in a completed Protocol implementation Conformance Statement (PICS) for IEEE Std 1609.2™-2016 in Annex B.1 – IEEE Std 1609.2 PICS.

Message Signed by Source
When the RSU is not the source of the message, but that message contains an IEEE Std 1609.2™-2016 signature of the source, the RSU shall verify the signature before broadcasting that message on the V2X interface.

Message Not Signed by Source
If the RSU is not the source of the message, the RSU shall verify the authorization of the source and the integrity of the received message. In addition, the RSU shall verify the plausibility of the data to the extent it is able to (See Section 4.3.5.2, Local and Back-Office Interface Security Design Details).

If these checks pass, then the RSU shall generate its own IEEE Std 1609.2™-2016 signature for that message, according to the security profile for that application (e.g. SPaT security profile).

If any of these checks do not pass, the RSU shall log the event locally in the system log defined by NTCIP 1218 v01 (Section 3.6.3.1) and not transmit any part of that message over the V2X interface.

4.3.5.1.2 Security - Receiving and Forwarding V2X Messages Design Details

The RSU shall fulfill the requirements specified in a completed Protocol implementation Conformance Statement (PICS) for IEEE Std 1609.2™-2016 in Annex B.1 – IEEE Std 1609.2 PICS, unless the RSU has a diagnostic setting enabled (See Section 4.3.1.3).

Whenever the RSU is configured to forward the messages it receives from OBUs/MUs over the V2X interface to other local or backend devices, the RSU shall verify the IEEE Std 1609.2™-2016 signed SPDUs containing the messages it intends to forward, per IEEE Std 1609.2™-2016 and the security profile for that application (e.g., BSM, SRM).

If the RSU is able to verify the IEEE Std 1609.2™-2016 signatures, then the RSU may forward the received message, with or without its verified signature, to the other local or backend devices.

If the RSU is unable to verify the IEEE Std 1609.2™-2016 signature, then the RSU shall log that event locally in the system log defined by NTCIP 1218 v01 (Section 3.6.3.1), but not forward the signature.

4.3.5.2 Local and Back-Office Interface Security Design Details

When setting up a TLS connection to another field device or a backend server to provide application services or data, the RSU shall use the TLS 1.3 protocol as specified in IETF RFC 8446 and employ a certificate acceptance policy, whether it is acting as a server or a client.

Exceptions to this are that the RSU is permitted to use any security protocol supported by the SCMS to connect to the SCMS, and that the RSU may use TLS 1.2 (as specified in IETF RTC 5246) to protect SNMPv3 connections if SNMPv3 over TLS 1.3 is unavailable.

The certificate acceptance policy shall be downloaded to the RSU as part of its initial configuration while in initialization mode, and shall require at a minimum that the TLS client uses a certificate. The certificate acceptance policy may include an allow-list of trusted server certificates and means to validate client certificates.

See 4.3.5.9.1, Assurance of Correct Initial Network Connection Design Details, where these certificates to be trusted are installed securely.

4.3.5.3 Data Integrity Design Details

Design Details not necessary.

4.3.5.4 Availability Design Details

Design Details not necessary.

4.3.5.5 Data Confidentiality Design Details

The RSU shall protect the management data by applying confidentiality services according to NTCIP 1218 v01 requirements 3.6.1.2.1 to 3.6.1.2.4, to incoming and outgoing management related messages. These requirements specify the use of:

- User-based Security Model (USM) for SNMPv3 (IETF RFC 3414, IETF RFC 5590)
- Transport Security Model (TSM) for SNMPv3 (IETF RFC 5591)
- Advanced Encryption Standard 256-bit (AES-256) keys (NIST FIPS PUB 197)
- Transportation Layer Security (TLS) Protocol (IETF RFC 6353)

Note: This protects data that is sensitive (for commercial or other reasons) from being revealed to unauthorized parties.

4.3.5.6 Tamper Evident Design Details

The security design details for tamper evidence follows.

4.3.5.6.1 Tamper Evident Enclosure - Visual Design Details

The RSU enclosure, along possible entry points to the RSU internal components, shall have ultraviolet-protected tamper-evident tape or sealing wax applied. This allows trained maintainers to determine whether an RSU enclosure has been opened.

4.3.5.6.2 Tamper Evident Port Design Details

Unused physical ports on the RSU shall be filled and then sealed with tamper-evident tape or sealing wax. This allows trained maintainers to determine whether an RSU physical port has been accessed.

4.3.5.7 Certificate Storage Design Details

The RSU contains a cryptographic storage module. The RSU shall adhere to the hardware security requirements described in the *CAMP Platform Security Document*.

4.3.5.8 RSU Operating System Security Design Details

The security design details for the RSU operating system follows.

4.3.5.8.1 RSU OS Applications and Services Design Details

By default, RSU applications that are not being utilized, shall SET NTCIP 1218 v01: 5.19.2.3, rsuAppConfigStartup to notStartup (3) for that application.

4.3.5.8.2 RSU OS Ports and Protocols Design Details

By default, the RSU operating system will block any incoming internet protocol (IP) transport layer port number that is not being actively used by an application or service on the RSU. The RSU shall adhere to the OS security requirements described in the *CAMP Platform Security Document*.

4.3.5.8.3 RSU Password Design Details

The RSU operating system shall come with the following password requirements in its OS password configuration file: (Refer to NIST 800-63B, Section 5.1.1, Memorized Secrets and *CIS Controls Implementation Guide for Industrial Control Systems*, Control 4 - Controlled Use of Administrative Privileges and Control 16 - Account Monitoring and Control).

- Password length for administrative account passwords shall be set to a minimum of 14 characters.
- Password length for non-administrative account passwords shall be set to a minimum of 8 characters.

Tasks requiring administrative accounts include:

- Install the public cert and private key.
- Install a chain of trust.
- Perform (re-)enrollment into an SCMS.
- Write/modify access control policies.
- Write/modify information flow control policies.
- Write the list of auditable activities.
- Delete audit log data.
- Install software other than signed software whose signature chains to a verification key whose integrity is protected by hardware on the device.

4.3.5.9 Connection Assurance Design Details

The security design details for connection assurance follows.

4.3.5.9.1 Assurance of Correct Initial Network Connection Design Details

As part of initial installation of an RSU on an operating agency network, the RSU shall be placed in an initialization mode whereby a user with administrator access can perform secure configuration of a TLS certificate.

The RSU shall support a vendor specific method whereby only an authorized administrator is able to configure a TLS certificate acceptance policy consisting of:

a) a chain of trust (i.e. All trusted Root and intermediate CAs)
b) an IOO-specific naming pattern for the SubjectAltName field in the client certificate to match (e.g., to distinguish between certs from the same Root CA but for different IOOs). The naming pattern shall support wildcards which can be used to allow all names with a certain suffix, e.g., "*.cityofnyc.gov".

4.3.5.9.2 Assurance of Continued Correct Network Connection Design Details

The RSU shall support verification that any TLS connection to the backend (TMS) is with the device whose valid certificate is stored in the allow-list of certificates.

The RSU shall support verification that any TLS connection to a local device (such as a TSC) is with the device whose certificate was validated as per the TLS certificate acceptancy policy of Design Detail 4.3.5.9.1, Assurance of Correct Initial Network Connection Design Details.

4.3.5.10 SCMS Design Details

The security design details for interfacing with an SCMS follows.

4.3.5.10.1 SCMS Enrollment Design Details

The design details for enrollment with an SCMS follows.

4.3.5.10.1.1 SCMS Bootstrap Design Details

The RSU shall have the following data securely installed onto it at the beginning of its lifecycle:

- All the SCMS Root Certificate Authorities (CA) certificates and elector certificates.
- The ECA (Enrollment Certificate Authority) certificate chain.
- The RA (Registration Authority) URL or FQDN (Fully Qualified Domain Name) and certificate chain, which could be one per each application.

4.3.5.10.1.2 SCMS Enrollment Design Details - CAMP

The RSU shall undergo manual enrollment as follows:

- The RSU shall be instructed to create an Enrollment Certificate Signing Request (CSR) (SignedEeEnrollmentCertRequest) according to https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/scms-protocol.asn?at=release/1.2.2), containing the PSID/SSPs for its authorized applications and the geographic region specifications it is authorized to use (circular or rectangular).
- The CSR shall be sent to the SCMS provider via a secure, authenticated method. For instance, this could be uploaded into a secure portal over TLS.
- The SCMS will return the enrollment certificate (SignedEeEnrollmentCertResponse) and the other bootstrap information referenced in Section 4.3.5.10.1.1 over a secure channel.
- The received bootstrap information and the enrollment certificate shall be downloaded into the RSU.

Note that, when this process is performed with an RSU that is already deployed in the field, this process shall use a secure connection between the RSU and the operator performing this process. This secure connection shall provide confidentiality, integrity protection, and authentication of the RSU. Note: Only authorized individuals use these connections to bootstrap the RSU.

4.3.5.10.1.3 SCMS Enrollment Design Details - IEEE Std 1609.2.1

The RSU supplier shall employ a secure environment for RSU enrollment, such that:

- Access to enrollment processes is limited to authorized personnel and equipment
- Only authorized devices are allowed to enroll, and a high-integrity and authenticated communication channel is used.
- Each RSU receives the correct credentials to operate with the infrastructure, that is, an enrollment certificate and one or more root CA certificates.
- The credentials are stored in RSU secure storage

Figure 15 depicts the manual enrollment provisioning for the IEEE Std 1609.2.1™-2020.

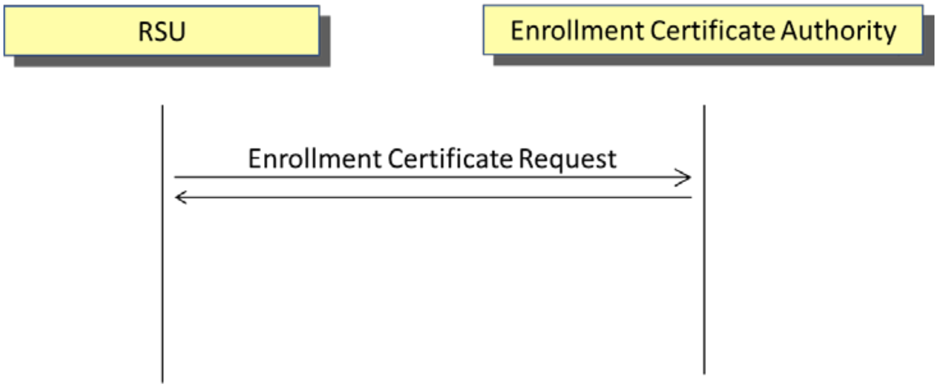

RSU
Enrollment Certificate Authority
Enrollment Certificate Request

Figure 15. Manual Enrollment Provisioning - IEEE Std 1609.2.1

High-level Design Details
The RSU shall send an enrollment certificate request message to the SCMS. The RSU shall use the SCMS REST API v2 as in Section 6.3.4.2 of IEEE Std 1609.2.1™-2020.

Details:
The RSU shall use an HTTPS connection and TLS v1.3 protocol to contact the ECA, as in Section 6.3.1.2. of IEEE Std 1609.2.1™-2020. The TLS implementation shall follow the recommendations in Section 5.3 of IEEE Std 1609.2.1™-2020.

4.3.5.10.2 SCMS Configurability Design Details

The RSU shall have the following data securely installed onto it by its administrator:

- The applications for which it can request application certificates from the SCMS. At a minimum, the applications are: WSA, SPaT, MAP, TIM, RSM and SSM.
- How often the process to request these application certificates from the SCMS shall be undertaken.

4.3.5.10.3 SCMS Connectivity Design Details

The design details for an RSU to connect with an SCMS follows.

4.3.5.10.3.1 SCMS Connectivity Design Details - CAMP

The RSU shall contact the provisioned RA to send a request for application/authorization certificate provisioning, using an HTTPS connection as in https://wiki.campllc.org/display/SCP/RA+-+Request+Application+Certificate+Provisioning.

The RSU shall contact the provisioned RA to send a download application/authorization certificate message, using an HTTPS connection as in https://wiki.campllc.org/display/SCP/RA+-+Download+Application+Certificate

The RSU shall be able to re-enroll to obtain a new enrollment certificate from the SCMS, in accordance to the *SCMS EE Certificate Rollover (Reenrollment) Technical Standard v01*.

4.3.5.10.3.2 SCMS Connectivity Design Details – IEEE Std 1609.2.1

High-level design details:
The RSU shall request and download application (authorization) certificates for itself from the SCMS. The RSU shall send the following messages, all according to the formats specified in Section 6.3.5 of IEEE Std 1609.2.1™-2020 (See Figure 16):

- Authorization certificate request
- Authorization certificate download

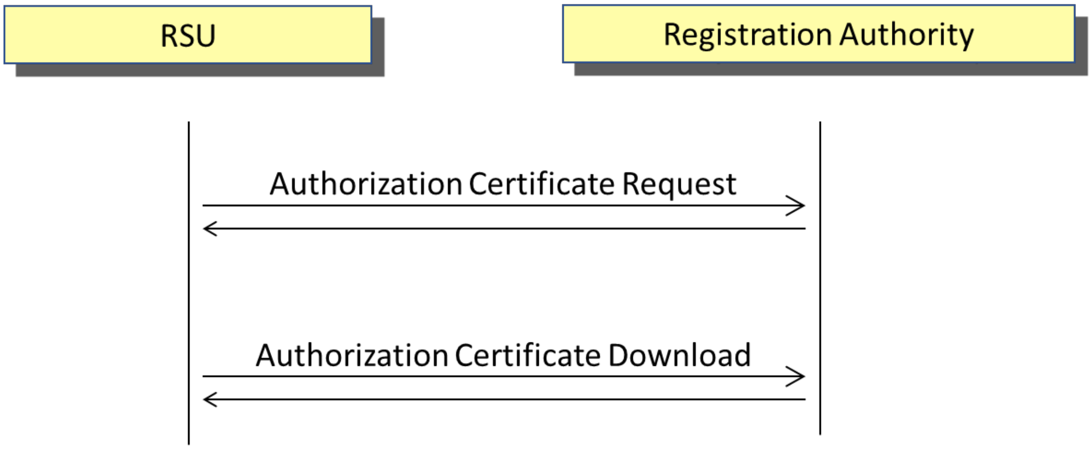

RSU
Registration Authority
Authorization Certificate Request
Authorization Certificate Download

Figure 16. Authorization Certificate Download - IEEE Std 1609.2.1

The RSU shall be able to send the following messages, all according to the formats specified in section 6.3.5 of IEEE Std 1609.2.1™-2020 (See Figure 17):

- Successor enrollment certificate request
- Successor enrollment certificate download

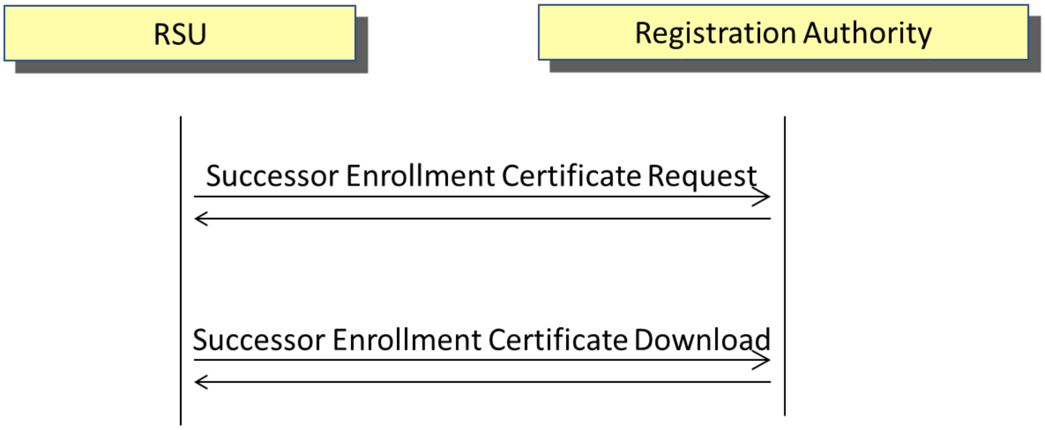

RSU
Registration Authority
Successor Enrollment Certificate Request
Successor Enrollment Certificate Download

Figure 17. Successor Enrollment Certificate Download – IEEE Std 1609.2.1

Details:
For all of the above messages, the RSU shall use the SCMS REST API v2 as in Section 6.3.4.2 of IEEE Std 1609.2.1™-2020.

The RSU shall use HTTPS connection and TLS 1.3 protocol to contact the provisioned Registration Authority, as in Section 6.3.1.2. of IEEE Std 1609.2.1™-2020. The TLS implementation shall follow the recommendations in Section 5.3 of IEEE Std 1609.2.1™-2020.

4.3.5.10.4 Certificate and Private Key Storage Design Details

The design for an RSU to store the SCMS related cryptographic material follows.

4.3.5.10.4.1 Key Storage Security Design Details

The RSU shall store all keys used to sign IEEE Std 1609.2™-2016 SPDUs within an HSM or hardware security equivalent to NIST FIPS 140-2 Level 3 physical security or higher.

4.3.5.10.4.2 Certificate Storage Design Details

The RSU shall protect its own certificates and SCMS component certificates used as trust anchors against modification, using mechanisms permitted by the *CAMP Platform Security document*.

4.3.5.10.4.3 Secure Platform Design Details

The RSU platform design shall follow the prescribed measures of the *CAMP Platform Security Document*.

Note: This platform design is expected to be incorporated into a future SAE J-series standard. SAE J3101_202002, Hardware Protected Security for Ground Vehicles was published in 2020. It is expected that the requirements for Hardware Protected Security in RSUs will be similar.

4.3.5.10.5 CRL Design Details

The design details for an RSU to download CRLs follow.

4.3.5.10.5.1 Download CRL Design Details - CAMP

The RSU shall download the CAMP SCMS CRL in accordance with the procedure provided at this link: https://wiki.campllc.org/display/SCP/MA+-+Download+CRL.

4.3.5.10.5.2 Download CRL Design Details- IEEE Std 1609.2.1

The RSU shall download any available CRLs from the provisioned RA, all according to the formats specified in Section 6.3.5 of IEEE Std 1609.2.1™-2020. These can be:

- Composite certificate revocation list download
- Individual CRL download

For each of the downloads, the RSU shall use the SCMS REST API v2 as in Section 6.3.4.2 of IEEE Std 1609.2.1™-2020.

The RSU shall use HTTPS connection with TLS v1.3 protocol to contact the provisioned Registration Authority, as in Section 6.3.1.2. of IEEE Std 1609.2.1™-2020. The TLS implementation shall follow the recommendations in Section 5.3 of IEEE Std 1609.2.1™-2020.

4.3.5.10.5.3 Update CRL and SCMS Files Design Details

For all CRLs that apply to messages the RSU might send or receive, the RSU shall attempt to update the CRL at least once a day for the week leading up to the nextCrl date given in that CRL.

4.3.5.10.6 Download SCMS Files Design Details

The design details for an RSU to download files from an SCMS follows.

4.3.5.10.6.1 Download SCMS Files Design Details - CAMP

The RSU shall download the Local Certificate Chain File (LCCF) and the Local Policy File (LPF) according to https://wiki.campllc.org/display/SCP/Step+13.3%3A+Download+RSE+Application+Certificate.

Note that this will be updated in the final guidance document: https://www.standards.its.dot.gov/.

4.3.5.10.6.2 Download SCMS Files Design Details- IEEE Std 1609.2.1

The RSU shall download the following system-wide security management data from the provisioned RA of the SCMS, all according to the formats specified in Section 6.3.5 of IEEE Std 1609.2.1™-2020.

- Certificate Chain File (CCF)
- Individual CA certificate download
- CTL download
- RA certificate download

For all of the above messages, the RSU shall use the SCMS REST API v2 as in Section 6.3.4.2 of IEEE Std 1609.2.1™-2020.

The RSU shall use HTTPS connection with TLS v1.3 protocol to contact the provisioned RA, as in Section 6.3.1.2. of IEEE Std 1609.2.1™-2020. The TLS implementation shall follow the recommendations in Section 5.3 of IEEE Std 1609.2.1™-2020.

4.3.5.11 Secure Administration Design Details

The RSU shall support management using SNMPv3 in accordance with NTCIP 1218 v01.

The RSU may support a web-based user access.

The RSU may support access by users via SSH.

The details for each of the above options follow.

4.3.5.11.1.1 Secure Administration – SNMPv3 Design Details

Communications with the RSU in accordance with NTCIP 1218 v01 shall be protected using TLS v1.2. This is an identified exception to Section 3.3.5.2, Local and Back-Office Interface Security Requirements, that communications shall be protected using TLS v1.3.

Note: SNMPv3 implemented by the RSU is currently defined over TLS v1.2. In the future, when this is upgraded to TLS v1.3, this requirement will be updated.

4.3.5.11.1.2 Secure Administration - Web-Based Access Design Details

If the RSU supports web-based user access, then the user may be authenticated by password or by a cryptographic mechanism.

If the user is authenticated by password, then:

- The RSU shall require that the user password is not the default password
- The RSU shall enforce that passwords meet the minimum strength under ‘RSU Password’ (See Section 4.3.5.8.3, RSU Password Design Details).

The web-based user access shall provide users with the ability to do only those tasks that are permitted by the user’s role. Users with administrative roles shall be required to use a strong password - see 4.3.5.8.3, RSU Password Design Details for definition of administrator activities and password strength.

4.3.5.11.1.3 Secure Administration – SSH Design Details

Communications with the RSU via SSH shall be protected using the SSH2 protocol. This is an identified exception to the statement in Section 3.3.5.2, Local and Back-Office Interface Security Requirements, that communications shall be protected using TLS v1.3.

If the RSU is being accessed by a user via SSH as defined in RFC 4253, then:

- No root access shall be available (root user shall be disabled)
- The RSU shall force a change from the default password on first login
- The RSU shall enforce that passwords meet the minimum strength under Section 4.3.5.8.3, RSU Password Design Details.
- The RSU shall only permit file copying via SCP (Secure Copy Protocol over SSH) or SFTP (SSH File Transfer Protocol). No other file copying protocol shall be permitted over SSH.

Note: SFTP is preferred to SCP.

The RSU shall support access control policy enabling assignment of what tasks can be carried out by users in different roles. Users with administrative roles shall be required to use a strong password - see 4.3.5.8.3, RSU Password Design Details for definition of administrator activities and password strength.

4.3.5.12 Secure Management of X.509 Credentials for TLS Design Details

The design details for the secure management of credentials follow.

4.3.5.12.1 Secure Interface for X.509 Credentials for TLS Design Details

The RSU shall support a secure, administrative interface by which:

- Its TLS signing certificate(s) may be installed or updated.
- Its trusted TLS Root CA may be configured or updated.
- An IOO-specific naming pattern for the SubjectAltName matching may be configured or updated.

4.3.5.12.2 Notification – X.509 Credentials for TLS Signing Certificate Design Details

The RSU can automatically send a notification that a TLS signing certificate is expiring within a configurable amount of time.

Note: The TMS may keep track of the expiration time of the RSU certificates.

4.3.5.12.3 Notification - X.509 Credentials for TLS Certificate Design Details

The RSU can automatically send a notification that an TLS certificate to trust is expiring within a configurable amount of time.

4.3.5.12.4 Expiration of Credentials Design Details

The RSU shall disconnect a TLS session at some point before the expiration of the TLS certificate (of either the RSU, the TMS or both) but after it receives the successor certificate, in accordance with NIST SP 1800-16 (Securing Web Transactions – TLS Server Certificate management).

4.3.5.13 Logging for General and Security Purposes Design Details

The RSU shall be able to be configured to support at the minimum, the following events:

- System startup and shutdown
- Service and application startup and shutdown
- Application failures/exceptions
- Application configuration changes (e.g., application security profile)
- Network connection and loss events (e.g., wireless or Ethernet connection)
- Modifications to security-related settings
- Successful and unsuccessful logon attempts
- Software and firmware updates
- Creation, modification and deletion of accounts and account privileges (users and apps)
- Accesses to files/directories used by software/firmware updates
- Unauthorized access attempts to corresponding private key operations (Optional)
- Network and firewall configuration changes
- Any changes to audit and audit reporting behavior
- Modifications to certificate trust lists
- Unauthorized attempts to modify log files

Otherwise, the design details for logging are vendor specific (e.g., the event messages).

4.3.5.14 Secure Update Design Details

The RSU shall implement the requirement 3.3.5.14 via a vendor-specific mechanism including:

- The RSU shall only install software and firmware updates which are signed by the RSU manufacturer.
- Update packages shall be authenticated by the RSU before installation.
- Unauthorized rollbacks to previous updates shall be prevented.

The RSU software update system shall protect software update authentication keys from compromise.

Annex A
Additional Notes [Informative]

A.1 Position Correction Messages

Position correction messages are useful for mobile-device applications that require precise position (e.g., lane-level accuracy). The immediate forward interface on the RSU (see Sections 2.5.2.8.1.1 and 2.5.2.8.1.2) can be used to send Radio Technical Commission for Maritime Services (RTCM) messages that are already formatted in conformance with SAE J2735_202007. RSU providers may choose to incorporate RTCM-related functionality natively on their RSU. This document does not require native RTCM functionality on the RSU, and this section is included for guidance purposes only.

Note: RTCMs can be obtained via Network Transport of RTCM via Internet Protocol (NTRIP), a Continuously Operating Reference Station (CORS), or other sources of positioning corrections.

A.2 Secure Sessions

When using IP-based communications between the OBU/MU and the back-office system, ISO/TS 21177:2109 using IEEE Std 1609.2™-2016 certificates or other forms of Transport Layer Security (TLS) can be used (e.g., X.509) to support secure sessions between the OBU/MU and back office. This should not require any special additional functionality on the RSU provided that IP is implemented by the RSU and corresponding routing is supported.

A.3 Wind Resistance Test

The RSU Specifications 4.1 contained a requirement for wind loading test (USDOT_RSU-Req_318-v001) that pointed to the AASHTO Standard Specifications for Structural Supports for Highway Signs, Luminaires, and Traffic Signals, Version 6 - Section 3.8. However, this reference was superseded by the publication of the AASHTO LRFD Specifications for Structural Supports for Highway Signs, Luminaires, and Traffic Signals, 1st Edition, 2015, also known as LRFDLTS-1. State agencies are encouraged to use this specification to design new signs, luminaires, etc.

Since structural requirements vary by agency, the RSU Standardization WG considered but ultimately agreed not to develop a requirement for wind loading and wind loading tests. These tests vary by agency and the environmental concerns for those agencies, based on each agency's individual criteria for wind loading and how it is mounted. The RSU Standardization WG encourages agencies consult their structural engineering departments on installations impacting existing supports.

Annex B
IEEE Std 1609 PICS [Normative]

In the following sections, items marked “Y” in the Support column are required and items marked “N” are optional. In some cases, a value is included to provide further guidance to implementers. Items marked N/A do not apply to the RSU security requirements.

These security PICS also represent minimum requirements, so an implementation can implement additional options as long as the default is implemented according to the Support column of the PICS presented in this Annex.

B.1 IEEE Std 1609.2 PICS

This section provides a protocol implementation conformance statement (PICS) from IEEE Std 1609.2™-2016 to specify the RSU security requirements. Implementers typically use a PICS to indicate compliance with particular features in the standard. The Item column contains a feature identifier; the Security configuration column contains a feature description; the Reference column contains the clause number for the IEEE Std 1609.2™-2016 standard, and the Status column indicates if the feature is mandatory or optional. Items marked with “M” are mandatory, and items marked with “O” are optional. Multiple items marked with O followed by a number (e.g., O1) indicate that the implementer chooses at least one of the options. Finally, items marked C followed by a number (e.g., C1) indicate that the implementer chooses one of the two features. The status column is part of the IEEE Std 1609.2™-2016 standard and cannot be modified. This document uses the Support column.

Table 23. IEEE Std 1609.2™-2016 Security Services Conformance Statement

Item	Security Configuration (Top-level)	Reference	Status	Support
S1.	Support Secure Data Service		O1	Y
S1.1.	Secure Data Exchange Entity (SDEE) Identification	4.2.2.1	0:M	Y
S1.1.1.	Support only one SDEE	4.2.2.1	0:C1	Distinguish between SDEEs
S1.1.2.	Distinguish between SDEEs	4.2.2.1	0:C1	
S1.2.	Generate SPDU		S1:O2	Y
S1.2.1.	Create Ieee1609Dot2Data containing Unsecured Data	4.2.2.2.2	S1.2:O3	N
S1.2.2.	Create Ieee1609Dot2Data containing valid SignedData	4.2.2.2.3, 5.2, 5.3.1, 5.3.3, 5.3.7, 6.3.4, 6.3.9, 9.3.9.1	S1.2:O3	Y
S1.2.2.1.	Using a valid HashAlgorithm	6.3.5	S1.2.2:M	Y
S1.2.2.1.1.	Support signing with hash algorithm SHA-256	6.3.5	S1.2.2:O3a	Y
S1.2.2.1.2.	Support signing with hash algorithm SHA-384	6.3.5	S1.2.2:O3a	N
S1.2.2.1.3.	Support signing with other hash algorithm	6.3.5	S1.2.2:O	N
S1.2.2.2.	Containing a Signed Data payload	6.3.6	S1.2.2:M	Y
S1.2.2.2.1.	… with payload containing data	6.3.7	S1.2.2.2:O4	Y
S1.2.2.2.2.	… with payload containing extDataHash	6.3.7	S1.2.2.2: O4	Y
S1.2.2.2.3.	… with generationTime in the security headers	6.3.9, 6.3.11	S1.2.2.2: O	Y
S1.2.2.2.4.	… with expiryTime in the security headers	6.3.9, 6.3.11	S1.2.2.2: O	Y
S1.2.2.2.5.	… with generationLocation in the security headers	6.3.9, 6.3.12	S1.2.2.2: O	Y

Item	Security Configuration (Top-level)	Reference	Status	Support
S1.2.2.2.6.	… with p2pcdLearningRequest in the security headers	6.3.9, 6.3.26	S1.2.2.2: O	N
S1.2.2.2.7.	… with missingCrlIdentifier in the security headers	6.3.9, 6.3.16	S1.2.2.2: O	N
S1.2.2.2.8.	… with encryptionKey in the security headers	6.3.9, 6.3.18	S1.2.2.2: O	Y
S1.2.2.2.8.1.	… … With a PublicEncryptionKey	6.3.9, 6.3.18, 6.3.19	S1.2.2.2.8: O5	Y
S1.2.2.2.8.2.	… … With a SymmetricEncryptionKey	6.3.9, 6.3.18, 6.3.20	S1.2.2.2.8: O5	N
S1.2.2.3.	Support a SignerIdentifier	6.3.25	S1.2.2:M	Y
S1.2.2.3.1.	… of type self	6.3.24	S1.2.2.3:O6	N
S1.2.2.3.2.	… of type digest	6.3.27	S1.2.2.3:O6	Y
S1.2.2.3.3.	… of type certificate	6.4.2	S1.2.2.3:O6	Y
S1.2.2.3.3.1.	… … Maximum number of certificates included in the SignerIdentifier	6.3.25	S1.2.2.3.2 1:M > 1:O	4
S1.2.2.4.	Support a Signature	6.3.28	S1.2.2:M	Y
S1.2.2.4.1.	… an ecdsa256Signature	6.3.29	S1.2.2.4:M	Y
S1.2.2.4.1.1.	… … using NIST p256	6.3.29	S1.2.2.4.1: O7	Y
S1.2.2.4.1.2.	… … using Brainpool p256r1	6.3.29	S1.2.2.4.1: O7	N
S1.2.2.4.1.3.	… … with a x-only r value	6.3.29	S1.2.2.4.1: O8	Y
S1.2.2.4.1.4.	… … with a compressed r value	6.3.29	S1.2.2.4.1: O8	
S1.2.2.4.1.5.	… … with an uncompressed r value	6.3.29	S1.2.2.4.1: O8	N
S1.2.2.4.1.6.	… an ecdsa384Signature using Brainpool p384r1	6.3.29a	S1.2.2.4:O6a	N
S1.2.2.4.1.7.	… … with a x-only r value	6.3.29a	S1.2.2.4.2: O8	N/A
S1.2.2.4.1.8.	… … with a compressed r value	6.3.29a	S1.2.2.4.2: O8	N/A
S1.2.2.4.1.9.	… … with an uncompressed r value	6.3.29a	S1.2.2.4.2: O8	N/A
S1.2.2.5.	Determine that certificate used to sign data is valid (part of a consistent chain, valid at the current time and location, has not been revoked)	5.2	S1.2.2:M	Y
S1.2.2.5.1.	Determine that the generation location is consistent with the region in the certificate	5.2.3.2.2, 6.4.17	S1.2.2.5:M	Y
S1.2.2.5.1.1.	Support a circularRegion	6.4.17, 6.4.18	S1.2.2.5.1: O9	Y
S1.2.2.5.1.2.	Support a rectangularRegion	6.4.17, 6.4.20	S1.2.2.5.1: O9	Y
	Maximum number of rectangularRegions supported	6.4.17, 6.4.20	S1.2.2.5.1.2 8:M > 8:O	8
S1.2.2.5.1.3.	Support a polygonalRegion	6.4.17, 6.4.21	S1.2.2.5.1: O9	Y

Item	Security Configuration (Top-level)	Reference	Status	Support
	Maximum number of points in a polygonalRegion	6.4.17, 6.4.21	S1.2.2.5.1.3 8:M > 8:O	Y
S1.2.2.5.1.4.	Support identifiedRegion	6.4.17, 6.4.22	S1.2.2.5.1: O9	Y
	Maximum number of identifiedRegions supported	6.4.17, 6.4.22	S1.2.2.5.1.4 : 8:M > 8:O	Y
	Support IdentifiedRegion of type CountryOnly	6.4.22, 6.4.23	S1.2.2.5.1.4 :O10	Y
	Support IdentifiedRegion of type CountryAndRegions	6.4.22, 6.4.24	S1.2.2.5.1.4 :O10	Y
	Support IdentifiedRegion of type CountryAndSubregions	6.4.22, 6.4.25	S1.2.2.5.1.4 :O10	Y
	List of supported IdentifiedRegions	5.2.3.4, 6.4.22	S1.2.2.5.1.4 :M	USA:Y
S1.2.2.5.2.	Determine that the certificate has the proper appPermissions	6.4.8, 6.4.28	S1.2.2.5:M	Y
S1.2.2.5.2.1.	Maximum number of PsidSsp in the appPermissions sequence	6.4.8, 6.4.28	S1.2.2.5.2 8:M > 8:O	8
S1.2.2.5.3.	Maximum supported length of the full chain (sending)	5.1.2.2	S1.2.2.5: 2:M >2:O	2 Note: The length of the full chain may be up to 8 but is recommended to be as short as possible.
S1.2.2.6.	Determine that key and certificate used to sign are a valid pair	5.3.7	S1.2.2:M	Y
S1.2.2.7.	Support signing with explicit certificates	6.4.6	S1.2.2.5:O11	N
S1.2.2.8.	Support signing with implicit certificates	5.3.2, 6.4.5	S1.2.2.5:O11	Y
S1.2.2.9.	Generate ECDSA keypairs using a high-quality random number generator	5.3.6	S1.2.2.4.1: M	Y
S1.2.3.	Create Ieee1609Dot2Data containing EncryptedData	4.2.2.3.2, 5.3.4, 6.3.30	S1.2:O2	Y
S1.3.	Receive SPDU		S1:O2	Y
S1.3.1.	Support preprocessing SPDUs	4.2.2.3.1	S1.3.2.3.1, S3.2 S3.3:M	Y
S1.3.2.	Verify Ieee1609Dot2Data containing SignedData	4.2.2.2.3, 5.2, 5.3.1, 5.3.3, 5.3.7, 6.3.4, 6.3.9	S1.3:O17	Y
S1.3.2.1.	Using a valid HashAlgorithm		S1.3.2:M	Y

Item	Security Configuration (Top-level)	Reference	Status	Support
S1.3.2.1.1.	Verify signed data using HashAlgorithm SHA-256	6.3.5	S1.3.2.1:O17a	Y
S1.3.2.1.2.	Verify signed data using a HashAlgorithm other than SHA-384	6.3.5	S1.3.2.1:O17a	N
S1.3.2.1.3.	Verify signed data using another HashAlgorithm	6.3.5	S1.3.2.1:O17a	N
S1.3.2.2.	Containing a Signed Data payload	6.3.6	S1.3.2:M	Y
S1.3.2.2.1.	… with payload containing data	6.3.7	S1.3.2.2:O18	Y
S1.3.2.2.2.	… with payload containing extDataHash	6.3.7	S1.3.2.2:O18	N
S1.3.2.2.3.	… with generationTime in the security headers	6.3.9, 6.3.11	S1.3.2.2:O	Y
S1.3.2.2.4	… with expiryTime in the security headers	6.3.9, 6.3.11	S1.3.2.2:O	N
S1.3.2.2.5	… with generationLocation in the security headers	6.3.9, 6.3.12	S1.3.2.2:O	N
S1.3.2.2.6.	… with missingCertIdentifier in the security headers	6.3.9, 6.3.24	S1.3.2.2:O	N
S1.3.2.2.7	… with missingCrlIdentifier in the security headers	6.3.9, 6.3.16	S1.3.2.2:O	N
S1.3.2.2.8	… with encryptionKey in the security headers	6.3.9, 6.3.18	S1.3.2.2:O	N
S1.3.2.2.8.1.	… … With a PublicEncryptionKey	6.3.9, 6.3.18, 6.3.19	S1.3.2.2.8: O19	N
S1.3.2.2.8.2.	… … With a SymmetricEncryptionKey	6.3.9, 6.3.18, 6.3.20	S1.3.2.2.8: O19	N
S1.3.2.3.	Support a SignerIdentifier	6.3.23	S1.3.2:M	Y
S1.3.2.3.1.	… of type self	6.3.24	S1.3.2.3:O20	N
S1.3.2.3.2.	… of type digest	6.3.25	S1.3.2.3:O20	Y
S1.3.2.3.3.	… of type certificate	6.4.2	S1.3.2.3:O20	Y
S1.3.2.3.3.1.	… … Maximum number of certificates included in the SignerIdentifier	6.3.25	S1.3.2.3.21:M > 1:O	1
S1.3.2.3.4.	… of type self		S1.3.2.3:O20	N
S1.3.2.4.	Support a Signature	6.3.28	S1.3.2:M	Y
S1.3.2.4.1.	… a ecdsa256Signature	6.3.30	S1.3.2.4:M	Y
S1.3.2.4.1.1.	… … using NIST p256	6.3.30	S1.3.2.4.1: O21	Y
S1.3.2.4.1.2.	… … using Brainpool p256r1	6.3.30	S1.3.2.4.1: O21	N
S1.3.2.4.1.3.	… … with a x-only r value	6.3.30	S1.3.2.4.1: O22	Y
S1.3.2.4.1.4.	… … with a compressed r value	6.3.30	S1.3.2.4.1: O22	Y
S1.3.2.4.1.5.	… … with a compressed r value and fast verification	6.3.30	S1.3.2.4.1: O22	N
S1.3.2.4.1.6.	… … with a uncompressed r value	6.3.30	S1.3.2.4.1: O22	N
S1.3.2.4.1.7.	… … with a uncompressed r value and fast verification	6.3.30	S1.3.2.4.1: O22	N

Item	Security Configuration (Top-level)	Reference	Status	Support
S1.3.2.4.2.	… a ecdsa384Signature using Brainpool p384r1	6.3.29	S1.3.2.4:M	N
S1.3.2.4.2.1.	… … with a x-only r value	6.3.29	S1.3.2.4.1: O22	N/A
S1.3.2.4.2.2.	… … with a compressed r value	6.3.29	S1.3.2.4.1: O22	N/A
S1.3.2.4.2.3.	… … with a compressed r value and fast verification	6.3.29	S1.3.2.4.1: O22	N/A
S1.3.2.4.2.4.	… … with a uncompressed r value	6.3.29	S1.3.2.4.1: O22	N/A
S1.3.2.4.2.5.	… … with a uncompressed r value and fast verification	6.3.29	S1.3.2.4.1: O22	N/A
S1.3.2.5.	SignedData verification fails if the certificate is not valid (part of a consistent chain, valid at the current time and location, has not been revoked)	5.2, 6.4.2	S1.3.2:M	Y
S1.3.2.5.1.	Reject data based on generation location being inconsistent with certificate	6.4.8, 6.4.17	S1.3.2.5:O	Y
S1.3.2.5.1.1.	… using a circularRegion	6.4.17, 6.4.18	S1.3.2.5.1: O23	Y
S1.3.2.5.1.2.	Support a rectangularRegion	6.4.17, 6.4.20	S1.3.2.5.1: O23	Y
S1.3.2.5.1.3.	Maximum number of rectangularRegions supported	6.4.17, 6.4.20	S1.3.2.5.1.2 8:M > 8:O	8
S1.3.2.5.1.4.	Support a polygonalRegion	6.4.17, 6.4.21	S1.3.2.5.1: O23	N
S1.3.2.5.1.5.	Maximum number of points in a polygonalRegion	6.4.17, 6.4.21	S1.3.2.5.1.4 8:M > 8:O	N
S1.3.2.5.1.6.	Support identifiedRegion	6.4.17, 6.4.22	S1.3.2.5.1 8:M > 8:O	N
	Maximum number of identifiedRegions supported	6.4.17, 6.4.22	S1.3.2.5.1.6: 8:M > 8:O	N/A
	Support IdentifiedRegion of type CountryOnly	6.4.22, 6.4.23	S1.3.2.5.1.6:O24	N/A
	Support IdentifiedRegion of type CountryAndRegions	6.4.22, 6.4.24	S1.3.2.5.1.6:O24	N/A
	Support IdentifiedRegion of type CountryAndSubregions	6.4.22, 6.4.25	S1.3.2.5.1.6:O24	N/A
S1.3.2.5.1.6.5.	List of supported IdentifiedRegions	6.4.17, 6.4.22	S1.2.2.5.1.4: M	N/A
S1.3.2.5.2.	Reject data if the certificate does not have the proper appPermissions	6.4.8, 6.4.28	S1.3.2.5:M	Y
S1.3.2.5.3.	Maximum number of PsidSsp in the appPermissions sequence	6.4.8, 6.4.28	S1.3.2.5 8:O > 8:O	8
S1.3.2.5.4.	Determine that the assuranceLevel is an acceptable level	6.4.8, 6.4.27	S1.3.2.5:O	N

Item	Security Configuration (Top-level)	Reference	Status	Support
S1.3.2.5.5.	Maximum length of the full chain (receiving)	5.1.2.2	S1.2.2.5: 2:M >2:O	8
S1.3.2.6.	Support verifying SPDUs signed with explicit authorization certificates	6.4.5	S1.3.2:O25	N
S1.3.2.7.	Support verifying SPDUs signed with implicit authorization certificates	5.3.2, 6.4.5	S1.3.2:O25	Y
S1.3.2.8.	Support explicit CA certificates	6.4.2, 6.4.6	S1.3.2:M	Y
S1.3.2.9.	Support receiving implicit CA certificates	6.4.2, 6.4.5	S1.3.2:O	N
S1.3.2.10.	SignedData verification fails in the following circumstances:	6.3.4	S1.3.2:M	Y
S1.3.2.10.1.	… SPDU-Parsing: Invalid Input	6.3.4	S1.3.2.10:M	Y
S1.3.2.10.2.	… SPDU-Parsing: Unsupported critical information field	6	S1.3.2.10:M	Y
S1.3.2.10.3.	… SPDU-Parsing: Certificate not found	4.3, 6.3.13, 6.3.14, 6.3.15	S1.3.2.10:M	Y
S1.3.2.10.4.	… SPDU-Parsing:Generation time not available	4.3, 6.3.13, 6.3.14, 6.3.15	S1.3.2.10:M	Y
S1.3.2.10.5.	… SPDU-Parsing:Generation location not available	4.3, 6.3.13, 6.3.14, 6.3.15	S1.3.2.10:M	Y
S1.3.2.10.6.	… SPDU-Certificate-Chain: Not enough information to construct chain	5.1.2	S1.3.2.10:M	Y
S1.3.2.10.7.	… SPDU-Certificate-Chain: Chain ended at untrusted root	5.1.2	S1.3.2.10:M	Y
S1.3.2.10.8.	… SPDU-Certificate-Chain: Chain was too long for implementation	5.1.2	S1.3.2.10:M	Y
S1.3.2.10.9.	… SPDU-Certificate-Chain: Certificate revoked	5.1.2	S1.3.2.10:M	Y
S1.3.2.10.10.	… SPDU-Certificate-Chain: Overdue CRL	5.1.2	S1.3.2.10:M	Y
S1.3.2.10.11.	… SPDU-Certificate-Chain: Inconsistent expiry times	5.1.2	S1.3.2.10:M	Y
S1.3.2.10.12.	… SPDU-Certificate-Chain: Inconsistent start times	5.1.2	S1.3.2.10:M	Y
S1.3.2.10.13.	… SPDU-Certificate-Chain: Inconsistant chain permissions	5.1.2	S1.3.2.10:M	Y
S1.3.2.10.14.	… SPDU-Crypto: Verification failure	5.3.1	S1.3.2.10:M	Y
S1.3.2.10.15.	… SPDU-Consistency: Future certificate at generation time	5.2.3	S1.3.2.10:M	Y
S1.3.2.10.16.	… SPDU-Consistency: Expired certificate at generation time	5.2.3	S1.3.2.10:M	Y
S1.3.2.10.17.	… SPDU-Consistency: Expiry date too early	5.2.3	S1.3.2.10:M	Y
S1.3.2.10.18.	… SPDU-Consistency: Expiry date too late	5.2.3	S1.3.2.10:M	Y
S1.3.2.10.19.	… SPDU-Consistency: Generation location outside validity region	5.2.3	S1.3.2.10:M	Y
S1.3.2.10.20.	… SPDU-Consistency: Unauthorized PSID	5.2.3	S1.3.2.10:M	Y
S1.3.2.10.21.	… SPDU-Internal-Consistency: Expiry time before generation time	6.4.8, 6.4.14, 5.2.3	S1.3.2.10:M	N/A
S1.3.2.10.22.	… SPDU-Internal-Consistency: extDataHash doesn't match	5.2.3	S1.3.2.10:M	Y
S1.3.2.10.23.	… SPDU-Local-Consistency: PSIDs don't match	5.2.3	S1.3.2.10:O	Y

Item	Security Configuration (Top-level)	Reference	Status	Support
S1.3.2.10.24.	… SPDU-Local-Consistency: Chain was too long for SDEE	5.2.3	S1.3.2.10:M	Y
S1.3.2.10.25.	… SPDU-Relevance: SPDU Too Old	5.2.4	S1.3.2.10:O	Y
S1.3.2.10.26.	… SPDU-Relevance: Future SPDU	5.2.4	S1.3.2.10:O	Y
S1.3.2.10.27.	… SPDU-Relevance: Expired SPDU	5.2.4	S1.3.2.10:O	N
S1.3.2.10.28.	… SPDU-Relevance: SPDU Too Distant	5.2.4	S1.3.2.10:O	N
S1.3.2.10.29.	… SPDU-Relevance: Replayed SPDU	5.2.4	S1.3.2.10:O	N
S1.3.3.	Decrypt Ieee1609Dot2Data containing EncryptedData	4.2.2.3.3, 5.3.5, 6.3.32	S1.3:O17	N

Table 24. IEEE Std 1609.2™-2016 CRL Verification Entity Conformance Statement

Item	Security Configuration (Top-level)	Reference	Status	Support
S2.	Support CRL Validation Entity	7	O1	Y
S2.1.	Correctly verify received CRL	7.4	S2:M	Y
S2.1.1.	…using hash ID-based revocation	5.1.3.5	S2.1:O29	Y
S2.1.1.1.	… of type fullHashCrl	7.3.2	S2.1.1:M	Y
S2.1.1.2.	… of type deltaHashCrl	7.3.2	O	N
S2.1.2.	… using linkage-based revocation	5.1.3.4	S2.1:O29	Y
S2.1.2.1.	… of type fullLinkedCrl	7.3.2	S2.1.2:M	Y
S2.1.2.2.	… of type deltaLinkedCrl	7.3.2	O	N
S2.1.2.3.	… containing individual linkage values	7.3.6	S2.1.2:M	Y
S2.1.2.4.	… containing group linkage values	7.3.6	O	Y

Table 25. IEEE Std 1609.2™-2016 Peer-to-Peer Certificate Distribution Conformance Statement

Item	Security Configuration (Top-level)	Reference	Status	Support
S3.	Support Peer to Peer Certificate Distribution (P2PCD)	8	O	N
S3.1.	Number of supported SDEEs	8.2.6	S3.2: 1:O > 1:O	N/A
S3.2.	Support out-of-band P2PCD operations	8	S3:O30	N/A
S3.3.	Support SSME and SDS operations for out-of-band P2PCD in the requester role	8.2.4.1.1	S3:O30	N/A
S3.3.1.	Under at least one condition, trigger request processing on receiving a trigger SPDU	8.2.4.1.1	S3.3:M	N/A
S3.3.2.	Do not trigger request processing on receiving a trigger SPDU for which a request is already active	8.2.4.1.1	S3.3:M	N/A
S3.3.3.	Number of simultaneously active P2PCD learning requests	8.2.4.1.1	S3.3: 1:O > 1:O	N/A
S3.3.4.	When request processing is triggered, include a P2PCD learning request in the next SPDU for the trigger SDEE except in the following exception cases	8.2.4.1.1, 8.2.6	S3.3: M	N/A

Item	Security Configuration (Top-level)	Reference	Status	Support
S3.3.4.1 .	Do not include a P2PCD learning request if a learning request for the same certificate has been received within p2pcd_observedRequestTimeout	8.2.4.1.1	S3.3.4:O	N/A
S3.3.4.2 .	Only include one P2PCD learning request no matter how many learning requests have been triggered	8.2.4.1.1	S3.3.4: M	N/A
S3.3.5	Receive notifications from a P2PCDE that a P2PCD learning response has been received and use those to update the list of known certificates	8.2.4.1.1	S3.3: M	N/A
S3.4.	Support SSME and SDS operations for out-of-band P2PCD in the responder role	8.2.4.2.2	S3:O30	N/A
S3.4.1.	Trigger response processing on receiving a P2PCD learning request	8.2.4.2.2	S3.4:M	N/A
S3.4.2.	Number of simultaneously active P2PCD learning responses	8.2.4.2.2, 8.2.6	S3.4: 1:O > 1:O	N/A
S3.4.3.	Do not trigger response processing if less than p2pcd_responseActiveTimeout has passed since last triggered	8.2.4.2.2	S3.4: M	N/A
S3.4.4.	Trigger sending response after random back-off time unless threshold number of responses have been observed	8.2.4.2.2	S3.4: M	N/A
S3.4.5.	Increment number of responses observed based on input from P2PCDE	8.2.4.2.2	S3.4: M	N/A
S3.5.	Support P2PCDE operations for P2PCD	8.2.4.2.2	S3:O30	N/A
S3.5.1.	Receive responses and provide to SSME	8.2.4.1.2, 8.2.4.2.2, 8.3.1	S3.5: M	N/A
S3.5.2.	Send responses when triggered by SSME	8.2.4.2.2, 8.3.1	S3.5: O	N/A
S3.5.3.	Send responses over WSMP	8.2.4.2.2	S3.5.2: M	N/A
S3.6.	Support inline P2PCD operations	8	S3:O30	N/A

B.2 IEEE Std 1609.3 PICS

This section provides a protocol implementation conformance statement (PICS) from IEEE Std 1609.3™-2020 to specify the Networking services requirements. Implementers typically use a PICS to indicate compliance with particular features in the standard. The Item column contains a feature identifier; the Security configuration column contains a feature description; the Reference column contains the clause number for the 1609.3 standard, and the Status column indicates if the feature is mandatory or optional. Items marked with “M” are mandatory, and items marked with “O” are optional. Multiple items marked with O followed by a number (e.g., O1) indicate that the implementer chooses at least one of the options. Finally, items marked C followed by a number (e.g., C1) indicate that the implementer chooses one of the two features. The status column is part of the IEEE Std 1609.3™-2020 standard and cannot be modified. This document uses the Support column.

Reference: IEEE Std 1609.3™-2020.

Table 26. PICS Proforma for 802.11 as Underlying Communication Technology

Item	Feature	Value	Reference	Status	Support
N1.	DATA PLANE		—	—	
N1.1.	LLC		5.2	M	Y
N1.1.1.	LLC extensions for WSMP		7.5	N1.3:M	Y
N1.2	IPv6		5.3, 6.4	O1	Y
N1.2.1.	Use stateless configuration		6.4	O	Y
N1.2.2.	Send IP datagrams		5.3	O2	Y
N1.2.3	Receive IP datagrams		5.3	O2	Y
N1.2.3.1.	Receive by link-local address		6.4	M	Y
N1.2.3.2.	Receive by global address		6.4	M	Y
N1.2.3.3.	Receive by host multicast addresses		6.4	O3	Y
N1.2.3.4.	Receive by router multicast addresses		6.4	O3	Y
N1.2.4.	UDP		5.4	O	Y
N1.2.5.	TCP		5.4	O	Y
N1.2.6.	Other IETF protocols	( )[a]	5.4	O	N
N1.3	WSMP		5.5	O1	Y
N1.3.1	WSM reception		5.5.3	O4	Y
N1.3.1.1.	Check WSMP Version number	( )[b]	5.5.3, 8.3.2	M	Y
N1.3.1.2.	Check Subtype field	( )[r]	5.5.3, 8.3.2	M	Y
N1.3.1.3.	Check TPID field	( )[s]	5.5.3, 8.3.2	M	Y
N1.3.1.4.	WAVE Info Elem Extension field		8.1.1	M	Y
N1.3.1.5.	Deliver message based on Address Info (PSID)		5.5.3	M	Y
N1.3.2.	WSM transmission		5.5.2	O4	Y
N1.3.2.1.	Insert WSMP Version number		8.3.2	M	Y
N1.3.2.2.	Insert Address Info (PSID)		8.3.3	M	Y
N1.3.2.3.	Outbound message size	( )[c]	5.5.2	M	Y
N1.3.2.3.	Transmit channel number		8.3.4.2	O	N*
N1.3.2.5.	Transmit data rate		8.3.4.3	O	N*
N1.3.2.6.	Transmit Power Used		8.3.4.4	O	N*
N1.3.2.7.	Channel Load		8.3.4.5	O	N
N1.3.2.8.	Insert Subtype features	( )[r]	8.3.2	M	Y
N1.3.2.9.	Insert TPID features	( )[s]	8.3.2	M	Y
N2.	MANAGEMENT PLANE		—	—	
N2.1.	User role		6.2.1	O	N
N2.1.1.	Receive WSAs over WSMP		6.3.2	O5	N/A
N2.1.2.	Verify and accept Secured WSA		6.3.3, 8.2.1	O5	N/A
N2.1.3.	Accept Unsecured WSA		6.3.3, 8.2.1	O5	N/A
N2.1.4.	WAVE Info Elem Extension fields		8.1.1	M	N/A
N2.1.5.	Calculate avail service link quality		6.3.4	O	N/A
N2.1.6.	WSA header		8.2.2	M	N/A
N2.1.6.1.	Check WSA Version number	( )[d]	8.2.2.2	M	N/A
N2.1.6.2.	Check WSA Identifier		8.2.2.4	O	N/A
N2.1.6.3.	Check Content Count		8.2.2.5	O	N/A
N2.1.6.4.	WSA header Info Element Ext field		8.2.2.6	M	N/A
N2.1.6.4.1.	Repeat Rate		8.2.2.6.1	O	N/A
N2.1.6.4.2.	2DLocation		8.2.2.6.2	O	N/A
N2.1.6.4.3.	3DLocation		8.2.2.6.3	O	N/A
N2.1.6.4.4.	Advertiser Identifier		8.2.2.6.4	O	N/A
N2.1.6.4.5.	Other info elements	( )[e]	8.2.2.6	O	N/A

Item	Feature	Value	Reference	Status	Support
N2.1.7.	Service Info Segment		8.2.3	M	N/A
N2.1.7.1.	Number of Service Info Instances	( )[f]	8.2.3	M	N/A
N2.1.7.2.	WAVE Information Element Extension		8.2.3.5	M	N/A
N2.1.7.2.1.	PSC		8.2.3.5.1	O	N/A
N2.1.7.2.2.	IPv6 Address		8.2.3.5.2	O	N/A
N2.1.7.2.3.	Service Port		8.2.3.5.3	O	N/A
N2.1.7.2.4.	Provider MAC Address		8.2.3.5.4	O	N/A
N2.1.7.2.5.	RCPI Threshold		8.2.3.5.5	O	N/A
N2.1.7.2.6.	WSA Count Threshold		8.2.3.5.6	O	N/A
N2.1.7.6.1.	WSA Count Threshold Interval		8.2.3.5.7	O	N/A
N2.1.7.6.2.	Alternate Interface Info		8.2.3.5.8	O	N/A
N2.1.7.2.7.	Other info elements	( )[g]	8.2.3.5	O	N/A
N2.1.8.	Channel Info Segment		8.2.4	M	N/A
N2.1.8.1.	Number of Channel Info Instances	( )[h]	8.2.4	M	N/A
N2.1.8.2.	WAVE Info Elem Extension field		8.2.4.8	M	N/A
N2.1.8.2.1	EDCA Parameter Set		8.2.4.8.1	O	N/A
N2.1.8.2.2	Channel Access		8.2.4.8.2	O	N/A
N2.1.8.2.3	Other info elements	( )[i]	8.2.4.8	O	N/A
N2.1.9.	WAVE Router Advertisement		8.2.5.1	O	N/A
N2.1.9.1.	WAVE Info Elem Extension field		8.2.5.7	M	N/A
N2.1.9.1.1.	Secondary DNS		8.2.5.7.1	O	N/A
N2.1.9.1.2.	Gateway MAC Address		8.2.5.7.2	O	N/A
N2.1.9.1.3.	Other info elements	( )[j]	8.2.5.7	O	N/A
N2.2.	Provider role		6.2.1	O	Y
N2.2.1.	Send WSA over WSMP		6.2.3.3	M	Y
N2.2.1.1.	Send Secured WSA		6.2.4.2.1, 8.2.1	O6	Y
N2.2.1.2.	Send Unsecured WSA		6.2.4.2.1, 8.2.1	O6	N
N2.2.2.	Send repeated advertisements		6.2.4.2.1	O	Y
N2.2.3.	Change ongoing advertisements		6.2.2.2, 6.2.4.2.2	O	Y
N2.2.4.	Delete service		6.2.3.6	O	Y
N2.2.5	WSA header		8.2.2	M	Y
N2.2.5.1.	Set WSA Version		8.2.2.2	M	Y
N2.2.5.2.	Set WSA Identifier		8.2.2.4	M	Y
N2.2.5.3.	Set Content Count		8.2.2.5	M	Y
N2.2.6.	WSA header Info Element Ext field		8.2.2.6	M	Y
N2.2.6.1.	Repeat Rate		8.2.2.6.1	O	Y
N2.2.6.2.	2DLocation		8.2.2.6.2	O	Y
N2.2.6.3.	3DLocation		8.2.2.6.3	O	Y
N2.2.6.4.	Advertiser Identifier		8.2.2.6.4	O	Y
N2.2.6.5.	Other info elements	( )[k]	8.2.2.6	O	Y
N2.2.7.	Service Info Segment		8.2.3	M	Y
N2.2.8.	Number of Service Info Instances	( )[l]	8.2.3	M	Y
N2.2.9.	WAVE Info Elem Extension field		8.2.3.5	O	Y
N2.2.9.1.	PSC		8.2.3.5.1	O	Y
N2.2.9.2.	IPv6 Address		8.2.3.5.2	O	Y
N2.2.9.3.	Service Port		8.2.3.5.3	O	Y
N2.2.9.4.	Provider MAC Address		8.2.3.5.4	O	Y
N2.2.9.5.	RCPI Threshold		8.2.3.5.5	O	Y
N2.2.9.6.	WSA Count Threshold		8.2.3.5.6	O	Y
N2.2.9.6.1.	WSA Count Threshold Interval		8.2.3.5.7	O	Y
N2.2.9.6.2.	Alternate Interface Info		8.2.3.5.8	O	Y

Item	Feature	Value	Reference	Status	Support
N2.2.9.7.	Other info elements	( )[m]	8.2.3.5	O	Y
N2.2.10.	Channel Info Segment		8.2.4	M	Y
N2.2.11.	Number of Channel Info Instances	( )[n]	8.2.4	M	Y
N2.2.12.	WAVE Info Elem Extension field		8.2.4.8	O	Y
N2.2.12.1.	EDCA Parameter Set		8.2.4.8.1	O	Y
N2.2.12.2.	Channel Access		8.2.4.8.2	O	Y
N2.2.12.3.	Other info elements	( )[o]	8.2.4.8	O	Y
N2.2.13.	Send WRA		8.2.5	O	Y
N2.2.13.1.	WAVE Info Elem Extension field		8.2.5.7	O	Y
N2.2.13.1.1.	Secondary DNS		8.2.5.7.1	O	Y
N2.2.13.1.2.	Gateway MAC address		8.2.5.7.2	O	Y
N2.2.13.1.3.	Other info elements	( )[p]	8.2.5.7	O	Y
N2.3.	Timing advertisement		—		N
N2.3.1.	Timing Advertisement generation		6.2.4.3	O	N/A
N2.4.	MIB maintenance		6.5	—	
N2.4.1.	Managed WAVE device		6.5	O	Y
N2.4.2.	MIB per standard		6.5	N.2.4.1:M	Y
N2.4.3.	Other MIB	( )[q]	6.5	O	Y

[a]List protocols supported.
[b]List version numbers supported.
[c]Enter maximum WAVE Short Message length.
[d]List version numbers supported.
[e]List any other WSA header WAVE Information Elements processed on reception.
[f]Enter maximum number of Service Info Instances processed on reception.
[g]List any other Service Info Segment WAVE Information Elements processed on reception.
[h]Enter maximum number of Channel Info Instances processed on reception.
[i]List any other Channel Info Segment WAVE Information Elements processed on reception.
[j]List any other WAVE routing advertisement WAVE Information Elements processed on reception.
[k]List any other WSA header WAVE Information Elements supported on transmission.
[l]Enter maximum number of Service Info Instances supported on transmission.
[m]List any other Service Info Segment WAVE Information Elements supported on transmission.
[n]Enter maximum number of Channel Info Instances supported on transmission.
[o]List any other Channel Info Segment WAVE Information Elements supported on transmission.
[p]List any other WAVE routing advertisement WAVE Information Elements supported on transmission.
[q]List any other MIBs supported.
[r]List Subtype values supported.
[s]List TPID values supported.
* These can be used in diagnostic mode.

Table 27. PICS proforma for LTE-V2X as Underlying Communications Technology

Item	Feature	Value	Reference	Status	Support
N3.	DATA PLANE		—	—	
N3.1.	Access Stratum		M.3.2	M	Y
N3.1.1.	Service access point for AS		M.5.2	N3.3:M	Y
N3.2.	IPv6		5.3, 6.4	O1	Y
N3.2.1.	Use stateless configuration		6.4	O	Y
N3.2.2.	Send IP datagrams		5.3	O2	Y
N.3.2.3.	Receive IP datagrams		5.3	O2	Y
N3.2.3.1.	Receive by link-local address		6.4	M	Y
N3.2.3.2.	Receive by global address		6.4	M	Y

Item	Feature	Value	Reference	Status	Support
N3.2.3.3.	Receive by host multicast addresses		6.4	O3	Y
N3.2.3.4.	Receive by router multicast addresses		6.4	O3	Y
N3.2.4.	UDP		5.4	O	Y
N3.2.5.	TCP		5.4	O	Y
N3.2.6.	Other IETF protocols	( )[a]	5.4	O	N
N3.3.	WSMP		5.5	O1	Y
N3.3.1.	WSM reception		5.5.3	O4	Y
N3.3.1.1.	Check WSMP Version number	( )[b]	5.5.3, 8.3.2	M	Y
N3.3.1.2.	Check Subtype field	( )[r]	5.5.3, 8.3.2	M	Y
N3.3.1.3.	Check TPID field	( )[s]	5.5.3, 8.3.2	M	Y
N3.3.1.4.	WAVE Info Elem Extension field		8.1.1	M	Y
N3.3.1.5.	Deliver message based on Address Info (PSID)		5.5.3	M	Y
N3.3.2.	WSM transmission		5.5.2	O4	Y
N3.3.2.1.	Insert WSMP Version number		8.3.2	M	Y
N3.3.2.2.	Insert Address Info (PSID)		8.3.3	M	Y
N3.3.2.3.	Outbound message size	( )[c]	5.5.2	M	Y
N3.3.2.4.	Transmit data rate		8.3.4.3	O	N
N3.3.2.5.	Transmit Power Used		8.3.4.4	O	N
N3.3.2.6.	Compact Time Confidence		8.3.4.6	O	Y
N3.3.2.7.	Insert Subtype features	( )[r]	8.3.2	M	Y
N3.3.2.8.	Insert TPID features	( )[s]	8.3.2	M	Y
N4.	MANAGEMENT PLANE			—	
N4.1.	User role		6.2.1	O	N
N4.1.1.	Receive WSAs over WSMP		6.3.2	O5	N/A
N4.1.2.	Verify and accept Secured WSA		6.3.3, 8.2.1	O5	N/A
N4.1.3.	Accept Unsecured WSA		6.3.3, 8.2.1	O5	N/A
N4.1.4.	WAVE Info Elem Extension fields		8.1.1	M	N/A
N4.1.5.	Calculate avail service link quality		6.3.4	O	N/A
N4.1.6.	WSA header		8.2.2	M	N/A
N4.1.6.1.	Check WSA Version number	( )[d]	8.2.2.2	M	N/A
N4.1.6.2.	Check WSA Identifier		8.2.2.4	O	N/A
N4.1.6.3.	Check Content Count		8.2.2.5	O	N/A
N4.1.6.4.	WSA header Info Element Ext field		8.2.2.6	M	N/A
N4.1.6.4.1	Repeat Rate		8.2.2.6.1	O	N/A
N4.1.6.4.2.	2DLocation		8.2.2.6.2	O	N/A
N4.1.6.4.3.	3DLocation		8.2.2.6.3	O	N/A
N4.1.6.4.4.	Advertiser Identifier		8.2.2.6.4	O	N/A
N4.1.6.4.5.	Extended Channel Infos and Info		8.2.2.6.5 8.2.2.6.5.1	M	N/A
N4.1.6.4.6.	Other info elements	( )[e]	8.2.2.6	O	N/A
N4.1.7.	Service Info Segment		8.2.3	M	N/A
N4.1.7.1.	Number of Service Info Instances	( )[f]	8.2.3	M	N/A
N4.1.7.2.	WAVE Information Element Extension		8.2.3.5	M	N/A
N4.1.7.2.1.	PSC		8.2.3.5.1	O	N/A
N4.1.7.2.2.	IPv6 Address		8.2.3.5.2	O	N/A
N4.1.7.2.3.	Service Port		8.2.3.5.3	O	N/A
N4.1.7.2.4.	Provider MAC Address		M.6.3	O	N/A
N4.1.7.2.5.	WSA Count Threshold		8.2.3.5.6	O	N/A
N4.1.7.2.5.1.	WSA Count Threshold Interval		8.2.3.5.7	O	N/A

Item	Feature	Value	Reference	Status	Support
N4.1.7.2.6.	Other info elements	( )[g]	8.2.3.5	O	N/A
N4.1.8.	WAVE Router Advertisement		8.2.5.1	O	N/A
N4.1.8.1.	WAVE Info Elem Extension field		8.2.5.7	M	N/A
N4.1.8.1.1.	Secondary DNS		8.2.5.7.1	O	N/A
N4.1.8.1.2.	Gateway MAC Address		M.6.4	O	N/A
N4.1.8.1.3.	Other info elements	( )[j]	8.2.5.7	O	N/A
N4.2.	Provider role		6.2.1	O	Y
N4.2.1.	Send Service Advertisements over WSMP		6.2.3.3	M	Y
N4.2.1.1.	Send Secured WSA		6.2.4.2.1, 8.2.1	O6	Y
N4.2.1.2.	Send Unsecured WSA		6.2.4.2.1, 8.2.1	O6	Y
N4.2.2.	Send repeated advertisements		6.2.4.2.1	O	Y
N4.2.3.	Change ongoing advertisements		6.2.2.2, 6.2.4.2.2	O	Y
N4.2.4.	Delete service		6.2.3.6	O	Y
N4.2.5.	WSA header		8.2.2	M	Y
N4.2.5.1.	Set WSA Version		8.2.2.2	M	Y
N4.2.5.2.	Set WSA Identifier		8.2.2.4	M	Y
N4.2.5.3.	Set Content Count		8.2.2.5	M	Y
N4.2.6.	WSA header Info Element Ext field		8.2.2.6	M	Y
N4.2.6.1.	Repeat Rate		8.2.2.6.1	O	Y
N4.2.6.2.	2DLocation		8.2.2.6.2	O	Y
N4.2.6.3.	3DLocation		8.2.2.6.3	O	Y
N4.2.6.4.	Advertiser Identifier		8.2.2.6.4	O	Y
N4.2.6.5.	Extended Channel Infos and Info		8.2.2.6.5 8.2.2.6.5.1	M	Y
N4.2.6.6.	Other info elements	( )[k]	8.2.2.6	O	Y
N4.2.7.	Service Info Segment		8.2.3	M	Y
N4.2.8.	Number of Service Info Instances	( )[l]	8.2.3	M	Y
N4.2.9.	WAVE Info Elem Extension field		8.2.3.5	O	Y
N4.2.9.1.	PSC		8.2.3.5.1	O	Y
N4.2.9.2.	IPv6 Address		8.2.3.5.2	O	Y
N4.2.9.3.	Service Port		8.2.3.5.3	O	Y
N4.2.9.4.	Provider MAC Address		M.6.3	O	Y
N4.2.9.5.	WSA Count Threshold		8.2.3.5.6	O	Y
N4.2.9.5.1.	WSA Count Threshold Interval		8.2.3.5.7	O	Y
N4.2.9.6.	Other info elements	( )[m]	8.2.3.5.2.5.7	O	Y
N4.2.10.	Send WRA		8.2.5	O	Y
N4.2.10.1.	WAVE Info Elem Extension field		8.2.5.7	O	Y
N4.2.10.1.1.	Secondary DNS		8.2.5.7.1	O	Y
N4.2.10.1.2.	Gateway MAC address		M.6.4	O	Y
N4.2.10.1.3.	Other info elements	( )[p]	8.2.5.7	O	Y
N4.3.	Timing advertisement		-		
N4.3.1.	Timing Advertisement generation		6.2.4.3	O	N
N4.4.	MIB maintenance		6.5	—	
N4.4.1.	Managed WAVE device		6.5	O	Y
N4.4.2.	Other MIB	( )[q]	6.5	O	Y

[a] List protocols supported.

[b] List version numbers supported.

[c] Enter maximum WAVE Short Message length.

[d] List version numbers supported.

[e] List any other WSA header WAVE Information Elements processed on reception.

[f] Enter maximum number of Service Info Instances processed on reception.

[g] List any other Service Info Segment WAVE Information Elements processed on reception.
[h] Enter maximum number of Channel Info Instances processed on reception.
[i] List any other Channel Info Segment WAVE Information Elements processed on reception.
[j] List any other WAVE routing advertisement WAVE Information Elements processed on reception.
[k] List any other WSA header WAVE Information Elements supported on transmission.
[l] Enter maximum number of Service Info Instances supported on transmission.
[m] List any other Service Info Segment WAVE Information Elements supported on transmission.
[n] Enter maximum number of Channel Info Instances supported on transmission.
[o] List any other Channel Info Segment WAVE Information Elements supported on transmission.
[p] List any other WAVE routing advertisement WAVE Information Elements supported on transmission.
[q] List any other MIBs supported.
[r] List Subtype values supported.
[s] List TPID values supported.

B.3 IEEE Std 1609.4 PICS

This section provides a protocol implementation conformance statement (PICS) from IEEE Std 1609.4™-2016 to specify the Multi-Channel Operation requirements. Implementers typically use a PICS to indicate compliance with particular features in the standard. The Item column contains a feature identifier; the Security configuration column contains a feature description; the Reference column contains the clause number for IEEE Std 1609.4™-2016, and the Status column indicates if the feature is mandatory or optional. Items marked with “M” are mandatory, and items marked with “O” are optional. Multiple items marked with O followed by a number (e.g., O1) indicate that the implementer chooses at least one of the options. Finally, items marked C followed by a number (e.g., C1) indicate that the implementer chooses one of the two features. The status column is part of the IEEE Std 1609.4™-2016 standard and cannot be modified. This document uses the Support column.

Note that C-V2X interfaces do not use IEEE Std 1609.4™-2016; therefore, the requirements in this section apply only to DSRC.

Table 28. Protocol Implementation Conformance Statement (PICS) Proforma

Item	Feature	Value	Reference	Status	Support
M1.	OCBActivated communication		5.1	M	Y
M2.	Operation on CCH	( )[a]	5.2	O4	Y
M2.1.	Continuous CCH access		6.3.1	O	Y
M3.	Operation on SCH	( )[b]	5.2.1, 5.2.3	O4	Y
M3.1.	Continuous SCH access		6.3.1	O	Y
M4.	Mixed operation		5.2	O	Y
M4.1.	Immediate access		6.3.3	O	Y
M4.2.	Alternating access		6.3.2	O	Y
M4.2.1.	Use common time reference		5.2.2, 6.2.2	M	Y
M4.2.1.1.	Derive timing from GPS		6.2.3	O5	Y
M4.2.1.2.	Derive timing from Timing Advertisement frame		6.2.3	O5	N
M4.2.1.3.	Derive timing from other timing source	( )[c]	6.2.3	O5	Y
M4.2.2.	Guard interval on transmit		6.2.5	M	Y
M4.2.3.	Medium busy at end of guard interval		6.2.5	M	Y
M5.	Transmit		5.3.2	O2	Y
M5.1.	EDCA and user priority		5.4	M	Y
M5.2.	Cancel transmissions		5.3.2	O	N

Item	Feature	Value	Reference	Status	Support
M5.3.	Send TA		6.2.6	O	N
M5.4.	Send other IEEE Std 802.11 frames	( )[d]	6.4	O	N
M5.5.	Send WSM		5.3.3	O3	Y
M5.5.1.	Expiry time		5.3.3	O	N
M5.6.	Send IPv6		5.3.4	O3	Y
M5.6.1.	Send IPv6 on SCH only		5.2.3	M	Y
M6.	Receive		5.3.5	O2	Y
M6.1.	Receive TA		6.2.7	O	N
M6.2.	Receive WSM		5.3.3	O3	Y
M6.3.	Receive IPv6		5.3.4	O3	Y
M7.	Device readdressing		6.6	O	N
M8.	MIB maintenance		6.5	—	
M8.1.	Managed WAVE device		3.1, 6.5	O	Y
M8.2.	IEEE Std 1609.4 MIB per Annex F		6.5	M8.1: M	Y
M8.3.	Other MIB	( )[e]	6.5	O	Y

Note 1 - Entries in the Item column may be hierarchical. Thus, an entry of the form M<a>.<b> indicates the item is part of the group identified by the item M<a> where all members of the group are subject to the conditions of applicability of M<a> [i.e., features lower in the numbering hierarchy (M<a>.<b>) are only applicable if the next higher level feature (M <a>) is identified in the Conformance column as being present].
Note 2 - Parentheses in the Value column indicate the user should enter information as specified in the accompanying footnote.
Node 3 - An entry of the form <pred>:<S> in the Status column indicates that the status <S> applies if the item identified by <pred> is identified in the **Conformance** column as being present.
Note 4 - Valid status values in the Status column are M, O, O<n>, and C<n>. A status of M indicates a mandatory feature. A status of O indicates an optional feature. A status of O<n> indicates a mutual conditionality such that the feature is optional but that support of at least one of the items that have statue O<n> is mandatory. A status of C<n> indicates a mutual conditionality such that support of one and one only of the items that have status C<n> is mandatory.

[a] List supported control channel(s), including country and operating class.
[b] List supported service channel(s), including country and operating class.
[c] Indicate device’s timing source(s).
[d] Enter IEEE Std 802.11 management frames/service request primitives supported.
[e] Enter references to other management information bases supported.

Annex C
User Requests [Informative]

This Annex identifies features and requirements that were suggested for this standard, but are either supported by mechanisms that may not be readily obvious. As this RSU Standard uses USDOT's RSU Specifications v4.1 as an initial source, this Annex also identifies requirements in that Specification that were not included in RSU Standard.

C.1 Requirements in USDOT RSU Specification v4.1 Not Included

This section summarizes requirements in USDOT RSU Specification v4.1 that do not have similar requirements in this RSU Standard, or in NTCIP 1218 v01, which is a normative reference for the RSU Standard.

C.1.1 Shock and Vibration Tests

USDOT_RSU-Req_320-v001, USDOT_RSU-Req_551-v002. The RSU Standardization WG considered requiring the shock and vibration tests specified in USDOT RSU Specification v4.1. However, it was not clear what testing values in Tables B.1 and C.1 should be used to perform the tests. The RSU Standardization WG also considered the values called out in BS EN 50556:2018 Road Traffic Signal Systems for class AL, which specifies using IEC 60068-2-64:2008 test procedures for a frequency range from 5 to 500 Hz and specific g forces (at specific frequencies). The RSU Standardization WG decided that the shock and vibration tests specified (using NEMA TS 2-2016 as a reference) were sufficient.

C.1.2 Integrated GNSS Receiver

USDOT_RSU-Req_363-v001. The roadside unit shall include an integrated GNSS receiver (for positioning and UTC time).

The RSU Standardization WG considered this requirement but agreed that while positioning and time from a GNSS receiver was required (See Requirement 3.3.2.3.2.1), it was not a requirement that the GNSS receiver be integrated into the RSU.

C.1.3 RSU Master-Slave Set/RSU RF Coverage

The RSU Standardization WG considered a user need series to support of series of requirements (USDOT_RSU-Req_361, USDOT_RSU-Req_364, USDOT_RSU-Req_576, USDOT_RSU-Req_577, and USDOT_RSU-Req_580) in the RSU Specification v4.1 related to a RSU Set, where there was a requirement for a RSU Set "Master" or master/slave mode where multiple RSUs were configured to operate as a single functional unit to extend the DSRC coverage.

The RSU Standardization WG originally created a user need, called RSU RF Coverage to support this feature. The need was, "The RSU needs to be capable of increasing the range of RF coverage when the RF coverage environment is challenging. This enables a single application or set of applications to function when the RF coverage environment is challenging, such as a RSU positioned on one side of a Texas Diamond Interchange reaching OBUs located the other side of the interchange, or an embankment affecting the range of the RF broadcasts from an RSU." Further, the RSU Standardization WG created requirements that satisfied this user need, but decided that those requirements were unnecessary.

The RSU Standardization WG recommends that to extend the RF coverage for a location, a TMS, TSC or back-office system transmit to multiple RSUs for broadcasting messages. Multiple RSUs can also receive, then forward the messages to a TMS, TSC, or back-office system, where duplicate messages can be determined and handled.

C.1.4 GPS Legitimacy

USDOT_RSU-Req_613-v002. The roadside unit SHOULD evaluate GPS sub-frame data to indicate the legitimacy of the GPS data frame source.

The RSU Standardization WG considered this requirement but was unsure how a RSU would authenticate the legitimacy of a GPS data frame, particularly from a testing perspective. As such, until further research was performed on how authentication is performed, the RSU Standardization WG decided not to include this requirement.

C.1.5 Reliability

The RSU Standardization WG considered a requirement on Reliability. Reliability is represented in the RSU Specification V4.1 as Mean-Time-Between-Failure (MTBF) (USDOT_RSU-Req_340-v001) and as Availability (USDOT_RSU-Req_341-v002). The original requirement considered for the RSU Standard was "The RSU shall be designed to remain operational for an average 100,000 hours calculated using MIL-HDBK-217." However, research into MIL-HDBK-217 indicated that reference is outdated. The RSU Standardization WG then considered IEC 61709:2017 “Electric components - Reliability - Reference conditions for failure rates and stress models for conversion”, which has a comprehensive and systematic approach to defining and using data to measure reliability of a product. However, to select the correct sections of IEC 61709:2017 require additional research, so the requirement was removed at this time.

C.1.6 USDOT Situation Data Clearinghouse and Warehouse

The RSU Standard does not have any specific requirements to deposit Intersection Situation Data into the USDOT Situation Data Clearinghouse nor to retrieve traveler information messages from the USDOT Situation Data Warehouse. However, NTCIP 1218 v01 does provide functionality that allows data received by the RSU to be forwarded to a specified IP address.

C.2 Requirements Considered

The following requirements were suggested for the RSU Standard, but are not supported.

C.2.1 Precision Time Protocol (PTP)

The RSU Standardization WG discussed using Precision Time Protocol (PTP) as a secondary time source instead of Network Time Protocol (NTP). However, PTP requires a grandmaster clock and support for multi-casting, both of which are not currently common with DOTs. The RSU Standardization WG agreed that additional research would be needed.

C.2.2 Detect Misbehavior

The RSU Standardization WG discussed user needs and requirements to detect misbehavior. The user needs defined were:

- The RSU needs to report detected misbehavior via V2X communications within its wireless coverage area for selected misbehavior types. This feature allows the IOO to determine if an entity or malfunctioning device is behaving maliciously using V2X communications.
- The RSU needs to report detected misbehavior to the SCMS that it is enrolled with. This feature allows misbehaving devices to be put on a CRL (if verified by the SCMS) and to protect other OBUs/MUs.

Requirements were defined as follows:

- Detect Misbehavior Requirement. The RSU shall detect the misbehaviors in the messages received from the OBUs.
- Report Misbehavior Requirement - CAMP. The RSU shall report misbehaviors to the SCMS in accordance with the CAMP's requirements.
- Report Misbehavior Requirement - IEEE Std 1609.2.1. The RSU shall report misbehaviors to the SCMS in accordance with IEEE Std 1609.2.1™-2020.

Design details for the reporting misbehaviors were proposed as follows:

- The RSU shall send misbehavior reports to the configured RA using REST API over HTTPS over TCP/IP as detailed in Misbehavior Report and Application Specification for Connected Vehicle Pilot Deployment.
- The RSU shall send the message “Misbehavior report submission” to the configured RA according to the formats specified in Section 6.3.5 of IEEE Std 1609.2.1™-2020. The RSU shall use the SCMS REST API v2 as in Section 6.3.4.2 of IEEE Std 1609.2.1™-2020. The RSU shall use HTTPS connection and TLS protocol to contact the provisioned RA, as in Section 6.3.1.2. of IEEE Std 1609.2.1™-2020. Note: Forthcoming misbehavior reporting mechanisms may be added in the future as new V2X applications are added.

However, during the design phase, it was determined what constitutes a misbehavior isn't well-defined, so these user needs and requirements were removed.

C.2.3 Furnished Equipment

The RSU Standardization WG considered a requirement that the RSU furnished in conformance to this standard shall be new and used. However, the RSU Standardization WG agreed that this requirement is a procurement decision by the procuring agency and does not belong in this standard.

C.2.4 Support for Auxiliary Processing

The RSU Standardization WG considered a requirement to support an auxiliary device with additional processing power capacity for an RSU. This device may be used to process Basic Safety Messages for example. However, the RSU Standardization WG agreed not to include this requirement because how to interface with this auxiliary device in an interoperable or interchangeable manner cannot be defined at this time.

C.3 Proposed Changes to NTCIP 1218 v01

The following changes are proposed changes for NTCIP 1218 v01.

C.3.1 All PSIDs

It is recommended that a wildcard, 0xFFFFFFFF, be defined RsuPsidTC in NTCIP 1218 v01. RsuPsidTC is defined in the NTCIP 1218 v01 Management Information Base (MIB) as follows:

```
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))
```

NTCIP 1218 v01 uses RsuPsidTC in most cases as a single value to represent a specific application with a single PSID value. However, for two specific design details, it is desired to used RsuPsidTC as a wildcard to represent ANY PSID value. The two specific design cases are:

- 4.3.1.3.1, Diagnostic Setting – Forwarding Received Messages Design Details for the object rsuReceivedMsgPsid
- 4.3.1.3.2, Diagnostic Setting – Forwarding Transmitted Messages Design Details for the object rsuXmitMsgFwdingPsid

C.3.2 Diagnostic Settings

It is recommended that an object be added to NTCIP 1218 v01 to support a diagnostic setting, which disables signing messages which would otherwise be signed by the RSU based on other settings. When “diagnosticSigningDisabled” is set to “on”, the RSU shall transmit all WAVE messages with the IEEE Std 1609.2™-2016 header Ieee1609Dot2Data.unsecuredData. The default value for “diagnosticSigningDisabled” shall be “off”. See 4.3.1.3.3Diagnostic Setting – Transmitting without Signature Design Details.

The proposed object is:

```
diagnosticSigningDisabled OBJECT-TYPE
   SYNTAX INTEGER { off (0), on (1) }
   MAX-ACCESS read-create
   STATUS current
   DESCRIPTION "<Definition> When this object is set to ON (1), the RSU
        transmits all 'signed' WAVE messages as 'unsigned' messages. This
        setting overrides settings instructing the RSU to sign messages in
        other OIDs, for example rsuMsgRepeatOptions.secure (Bit 1) or
        rsuIFMOptions.secure (Bit 1). 'Unsigned' messages are transmitted
        with the IEEE Std 1609.2 header Ieee1609Dot2Data.unsecuredData.
   <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.22"
   DEFVAL {0}
::= { rsuSysSettings 22 }
```

The RSU Standardization WG also considered creating an object definition to limit the time duration that the RSU may remain in this diagnostic setting (in hours), but the RSU Standardization WG agreed to defer this to the NTCIP 1218 v01 working group.

C.3.3 Log Interface Filename

It is recommended that rsuIfaceLogName be changed from a MAX-ACCESS of read-create to a MAX-ACCESS of read-only. Based on the description in NTCIP 1218 v01 for rsuIfaceLogName, the filename is auto-generated by the RSU so a client cannot set the filename, so this object should be read-only.

C.3.4 Support for Factory Default

It is recommended that the NTCIP RSU Working Group consider adding support in NTCIP 1218 v01 to allow a management station to reboot the RSU to the last saved values, user-configured default settings, or to its factory default settings (See Sections 3.3.2.2.1 to 3.3.2.2.3).

C.3.5 Additional Support for Forwarding Messages Received by the RSU

It is recommended that the NTCIP RSU Working Group consider adding support in NTCIP 1218 v01 to allow the RSU to use TCP or a Virtual Private Network (VPN) to forward the messages received by the RSU over the V2X Interface. Security requirements have disallowed DTLS and UDP, thus an alternate method is needed.

C.3.6 Support for BSM Filtering

It is recommended that the NTCIP RSU Working Group consider the following object definitions to support BSM Filtering. The design details for BSM Filtering can be found in Section 4.3.2.14.4.

```
rsuZoneEvent OBJECT IDENTIFIER ::= { rsu 21 }

RsuZoneEventMsg ::= SEQUENCE {
    -- version for future enhancements
    version                            INTEGER { v1(1) },
    -- ID of zone where event happened
    rsuZoneEventSubscrZoneID           Integer32 (1..16),
    -- Type of zone event, e.g. "ZoneEnter"
    rsuZoneEventSubscrEventType        DisplayString,
    -- signal strength of received message
    rssi                               Integer32 (-100..-60),
    -- indication of whether the received message was signed
    signature                          INTEGER { unsigned(0), signed(1) },
    -- payload of received message, either with or without security header
    -- depending on setting of rsuZoneEventSubscrSecure
    rsuZoneEventSubscrMsgPayload       OCTET STRING (SIZE(1..2302)) }

maxZoneEvent OBJECT-TYPE
    SYNTAX       Integer32 (1..255)
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "<Definition> The maximum number of zone event entries this
      Roadside Unit supports. This object indicates the maximum rows which
      appears in the rsuZoneEventTable object.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.21.1"
::= { rsuZoneEvent 1 }

rsuZoneEventTable OBJECT-TYPE
    SYNTAX SEQUENCE OF rsuZoneEventEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Contains the subscriptions to zone events
      being sent to a network host, the IP Address and port number of the
      destination host, as well as other configuration parameters as defined.
    <TableType>  static
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.21.2"
::= { rsuZoneEvent 2 }

rsuZoneEventEntry OBJECT-TYPE
    SYNTAX       RsuZoneEventEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> A row describing the RSU Zone Event Entry.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.21.2.1"
    INDEX        { rsuZoneEventSubscrIndex }
    ::= { rsuZoneEventTable 1 }

RsuZoneEventEntry ::= SEQUENCE {
    rsuZoneEventSubscrIndex              RsuTableIndex,
    rsuZoneEventSubscrZoneID             Integer32,
    rsuZoneEventSubscrEventType          DisplayString,
    rsuZoneEventSubscrDestIpAddr         DisplayString,
    rsuZoneEventSubscrDestPort           Integer32,
    rsuZoneEventSubscrProtocol           INTEGER,
    rsuZoneEventSubscrSecure             INTEGER,
    rsuZoneEventSubscrStatus             RowStatus     }

rsuZoneEventSubscrIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "<Definition> Zone events index. This value shall be less
      than the value of maxZoneEvent.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.21.2.1.1"
::= { rsuZoneEventEntry 1 }

rsuZoneEventSubscrZoneID OBJECT-TYPE
    SYNTAX       Integer32 (1..16)
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "<Definition> ID of zone where event happened
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.21.2.1.2"
::= { rsuZoneEventEntry 2 }

rsuZoneEventSubscrEventType OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..32))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION "<Definition> Type of zone event, e.g. 'ZoneEnter'
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.21.2.1.3"
::= { rsuZoneEventEntry 3 }

rsuZoneEventSubscrDestIpAddr OBJECT-TYPE
    SYNTAX       DisplayString (SIZE(0..64))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION "<Definition> Destination Server IP address to forward the
      zone events to. 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> 1.3.6.1.4.1.1206.4.2.18.21.2.1.4"
::= { rsuZoneEventEntry 4 }

rsuZoneEventSubscrDestPort OBJECT-TYPE
    SYNTAX       Integer32 (1024..65535)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "<Definition> Destination Server Port Number to forward zone
      events to.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.21.2.1.5"
```

```
::= { rsuZoneEventEntry 5 }

rsuZoneEventSubscrProtocol OBJECT-TYPE
    SYNTAX       INTEGER { other (1), udp (2) }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION "<Definition> Transport Protocol between RSU and Server to
      forward zone events to. 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> 1.3.6.1.4.1.1206.4.2.18.21.2.1.6"
    DEFVAL { udp }
::= { rsuZoneEventEntry 6 }

rsuZoneEventSubscrSecure 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.

      This payload is sent inside the rsuZoneEventSubscrMsgPayload field
      within the RsuZoneEventMsg.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.21.2.1.7"
::= { rsuZoneEventEntry 7 }

rsuZoneEventSubscrStatus OBJECT-TYPE
    SYNTAX       RowStatus
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION "<Definition> Create (4) and destroy (6) row entry.
    <Object Identifier> 1.3.6.1.4.1.1206.4.2.18.21.2.1.8"
::= { rsuZoneEventEntry 8 }
```

C.3.7 Support For PC5 Status

RSU Standard v01 identifies a requirement to Monitor the Current Status. Table 21 identifies NTCIP 1218 v01 objects and their expected values to fulfill this requirement, however, there is no current object definition in NTCIP 1218 that describes the status of the communications for C-V2X. It is recommended that the NTCIP RSU Working Group add a new object, e.g., rsuPc5Status, with values like OK, Suspended, and Error to represent the current status of C-V2X communications. Suspended indicates when GPS time accuracy is not sufficient for reliable communications.

§