Dedicated Short-Range Communications Roadside Unit Specifications

www.its.dot.gov/index.htm

April 28, 2017
FHWA-JPO-17-589

U.S. Department of Transportation

Produced under Saxton Transportation Operations Laboratory Task Order 07 (Revision to DSRC Roadside Equipment (RSE) Specification), DTFH61-12-D-00020-T-13007
U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology

Notice

Quality Assurance Statement

The Federal Highway Administration (FHWA) provides high-quality information to serve Government, industry, and the public in a manner that promotes public understanding. Standards and policies are used to ensure and maximize the quality, objectivity, utility, and integrity of its information. FHWA periodically reviews quality issues and adjusts its programs and processes to ensure continuous quality improvement.

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-JPO-17-589		

4. Title and Subtitle	5. Report Date
Dedicated Short Range Communications Roadside Unit Specifications	April 28, 2017
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Frank Perry, Kelli Raboy, Ed Leslie, Zhitong Huang, Drew Van Duren	

9. Performing Organization Name And Address	10. Work Unit No. (TRAIS)
Leidos 11251 Roger Bacon Drive Reston, VA 20190	11. Contract or Grant No.

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
U.S. Department of Transportation Federal Highway Administration Saxton Transportation Operations Laboratory 6300 Georgetown Pike McLean, VA 22101	Specification April 11, 2016 – October 31, 2016
	14. Sponsoring Agency Code HRDO

15. Supplementary Notes

Deb Curtis, GTM

16. Abstract

The Intelligent Transportation Systems (ITS) Program definition of connected vehicles includes both 5.9 Gigahertz (GHz) Dedicated Short Range Communications (DSRC) and non-DSRC technologies as means of facilitating communication for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) applications. Non-DSRC technologies (e.g. Radio Frequency Identification (RFID), Worldwide Interoperability for Microwave Access (WiMAX), Wi-Fi, Bluetooth, and cellular communication) enable use of existing commercial infrastructure for additional capacity support, but may not meet the low-latency needs of transmitting safety-critical information.

DSRC is a two-way wireless communications protocol suite that integrates the IEEE 802.11, 1609.x standards, SAE J2735, and SAE J2945. The United States Department of Transportation (USDOT) is pursuing DSRC because of its low-latency and high-reliability performance that can be used to reduce fatalities through active safety applications, including collision avoidance, incident reporting and management, emergency response, and pedestrian safety. Furthermore, DSRC supports the close-range communication requirements to distribute Signal Phase and Timing (SPaT) information for intersection-based applications and localized roadway warnings. This document will set the requirements for roadside units (RSU) capable of acting as a network edge device for 5.9GHz DSRC infrastructure.

17. Key Words	18. Distribution Statement
Dedicated Short Range Communication, DSRC, Roadside Unit, RSU, Roadside Equipment, RSE, Intelligent Transportation Systems, ITS, V2I	No restrictions.

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	126	N/A

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

Table of Contents

List of Tables

List of Figures

Chapter 1. Introduction

The Intelligent Transportation Systems (ITS) Program definition of connected vehicles includes both 5.9 Gigahertz (GHz) Dedicated Short Range Communications (DSRC) and non-DSRC technologies as means of facilitating communication for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) applications. Non-DSRC technologies (e.g. Radio Frequency Identification (RFID), Worldwide Interoperability for Microwave Access (WiMAX), Wi-Fi, Bluetooth, and cellular communication) enable use of existing commercial infrastructure for additional capacity support, but may not meet the low-latency needs of transmitting safety-critical information.

DSRC is a two-way wireless communications protocol suite that integrates the IEEE 802.11, 1609.x standards, SAE J2735, and SAE J2945. The United States Department of Transportation (USDOT) is pursuing DSRC because of its low-latency and high-reliability performance that can be used to reduce fatalities through active safety applications, including collision avoidance, incident reporting and management, emergency response, and pedestrian safety. Furthermore, DSRC supports the close-range communication requirements to distribute Signal Phase and Timing (SPaT) information for intersection-based applications and localized roadway warnings.

What Is the Purpose of this Document?

This document will set the requirements for roadside units (RSU) capable of acting as a network edge device for 5.9GHz DSRC infrastructure.

Who Should Read this Document?

Suppliers interested in building roadside devices for DSRC Infrastructure Systems.

How Is this Document Organized?

The Structure of this document is as follows:

- Section 1 – Introduction: Revision History and Roadside Unit Description
- Section 2 – Scope: System Overview, Document Overview, and References.
- Section 3 – System Requirements: Describes RSU Physical, Environmental, and Functional Requirements.

How Do You Receive More Information?

Additional information is available in the documents listed in section 2.4. Questions are answered by the person responsible for this document (see section 1.5).

Revision History

Table 1-1. Revision History.

Rev.	Ver.	Date	Description	Approved by	Responsible
4.0	2	05/15/2014	First Issue	Deb Curtis (FHWA)	
4.1	1	07/22/2016	Updates to reference current standards (SCMS EE Requirements v1.1, IEEE 802.11-2012 IEEE 1609.x-2016, SAE J2735-2016) as well as updates based on evaluations of 4.0 specification devices Added, updated, and removed various requirements for clarity and enhancement	Deb Curtis (FHWA)	Frank Perry, Kelli Raboy, Ed Leslie, Zhitong Huang
4.1	2	08/12/2016	Updates to address known security issues, health and monitoring functionality, and interface with the Situation Data Warehouse and Clearinghouse. New introductory section on the basic functionality of an RSU Modified Appendix B with draft revised MIB Added, updated, and removed various requirements for clarity and enhancement	Deb Curtis (FHWA)	Frank Perry, Kelli Raboy, Ed Leslie, Zhitong Huang, Drew Van Duren
4.1	3	08/31/2016	Updates to address stakeholder feedback, largely related to security issues and health and monitoring functionality. Modified Appendix B with revised MIB Added Appendix D: Example WAVE	Deb Curtis (FHWA)	Frank Perry, Kelli Raboy, Ed Leslie, Zhitong Huang, Drew Van Duren

Rev.	Ver.	Date	Description	Approved by	Responsible
			Service Advertisement (WSA)		
4.1	4	10/31/2016	Revised Figure 6 Modified Appendix B.1 with updated MIB Added Appendix B.4, a mapping of RSU specific MIB OIDs Updated Appendix D to provide a WSA example utilizing the latest standard Removed Section 3.7.1.2. and consolidated requirements into Section 3.7.1.1. Revised terms used throughout the document for clarity Added, updated, and removed various requirements for clarity and enhancement	Deb Curtis (FHWA)	Frank Perry, Kelli Raboy, Ed Leslie, Zhitong Huang, Drew Van Duren
4.1	5	1/20/2017	Reformatted the document to follow JPO guidelines Corrected errors in the MIB in Appendix B.1 Typographical errors were corrected in the following requirements: • Req_453-v002 • Req_319-v001 • Req_550-v002	Deb Curtis (FHWA)	Ed Leslie, Zhitong Huang, Lisa Bedsole, Andrea Vann-Easton

Roadside Units

DSRC enables communication between vehicles and roadside equipment, but does not generate data necessary to provide warnings and advisories from infrastructure to drivers. To support V2I applications, DSRC must be integrated with existing traffic equipment, such as Signal Controllers and backhaul connections to Traffic Management Centers (TMCs). DSRC devices that serve as the demarcation component between vehicles and other mobile devices and existing traffic equipment will be referred to DSRC Roadside Units (RSU) in this document.

Chapter 2. Scope

This document defines the fourth-generation of DSRC RSUs by establishing the base functionality of a carrier-grade device capable of acting as the infrastructure first point-of-contact for vehicles and other mobile devices.

A carrier-grade RSU is defined as an RSU in which both the hardware and software components operate un-attended in harsh outdoor environments (temperature and precipitation extremes) for extended periods of time (typical Mean-Time-Between-Failures (MTBF) of 100,000 hours). Individual RSUs as well as groups of RSUs can be managed and monitored with existing off-the-shelf network tools with minimal modifications to support RSU specific data elements; RSUs ignore erroneous, malformed, or unexpected data received on any of its interfaces, detect and auto-recover from minor software failures, transient power spikes, and unexpected power interruptions.

These requirements apply only to the system components identified in Section 2.1 System Overview and do not extend to the supporting roadside equipment subsystems or components. RSUs procured for deployment may be subject to additional requirements based on the local design and policies of the procuring agency.

System Overview

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

Figure 2-1 depicts a high-level diagram of the RSU and its role as a DSRC interface between traffic management infrastructure and vehicles and other mobile devices.

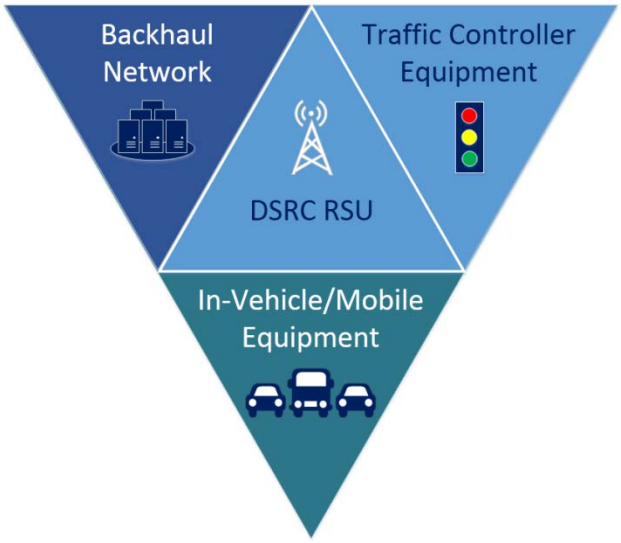

Figure 2-1. Diagram. High-level Conceptual Diagram for the Roadside Units.

The definition[1] of an RSU that complies with the requirements contained in this document is a device that:

- Supports Single Channel Continuous and dual Channel Alternating DSRC Channel Modes simultaneously.
- Contains internal computer processing and permanent storage capability.
- Contains an integrated Global Positioning System (GPS) receiver for positioning and timing.
- Contains a Power-over-Ethernet (PoE) capable interface that supports both IPv4 and IPv6 connectivity, compliant with IEEE 802.3at.
- Is contained in a dedicated, NEMA 4X-rated enclosure.

For this document, Single Channel Continuous Mode is defined as operating on a single radio channel through both Time Slot 0 and Time Slot 1 as defined in IEEE 1609.4. Dual Channel Alternating Mode is defined as operating on the Control Channel (CCH) during Time Slot 0 and on a Service Channel during Time Slot 1.

The RSU will have a set of operational states as illustrated in Figure 2-2, below.

[1] This definition is not intended to supersede FCC guidance for licensing and operation of an RSU; the FCC definition of an RSU can be found in the Electronic Code of Federal Regulations, Title 47: Telecommunications, Part 90 – Private Land Mobile Radio Services. http://www.ecfr.gov/cgi-bin/text-idx?SID=5ea03a4e0adab6bf55092d7fd90dd701&node=47:5.0.1.1.3&rgn=div5#47:5.0.1.1.3.12.113

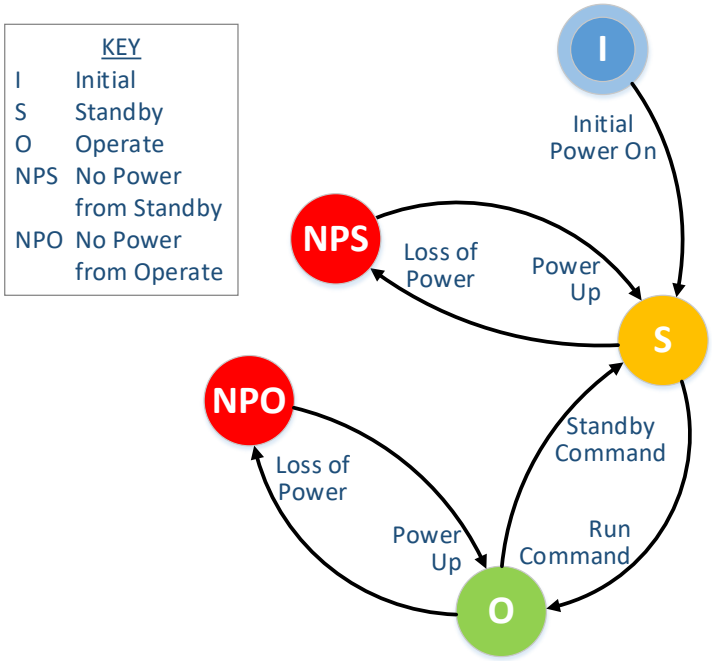

Figure 2-2. Diagram. Roadside Unit State.

Table 2-1. Operational States and State Transitions.

State	Definition
Initial	This is the initial state of the device from the factory, with no specified requirements. The device will revert to the "initial" state after a factory reset.
Standby	• Core Operating System is operational • DSRC radios are not operational/broadcasting • Interface logging is disabled; • Configuration changes are enabled
No Power Operate	This state results from a loss of power when the RSU is in the Operate State; this is **NOT** a graceful shutdown that would be enacted by a transition to Standby State prior to a transition to the No Power State.
No Power Standby	This state results from a loss of power when the RSU is in the Standby State. The unit should return to the Standby state upon power up.
Operate	• All DSRC radios are operational/broadcasting • System log is enabled • Configuration changes are disabled

The installation of the RSU is dependent upon local design, policies, and available infrastructure; an RSU can be mounted directly on a traffic pole or mast arm, or installed in an adjacent cabinet to ensure radio communication objectives can be met. This specification includes sufficient consideration of environmental exposure to cover all deployment configurations, with examples depicted in Figure 2-3 through Figure 2-5. The red boxes in these diagrams highlight the system components that are covered by this specification, including the RSU device and antennas, excluding supporting hardware and infrastructure such as gantries or mast arms and traffic controller or electronics cabinets.

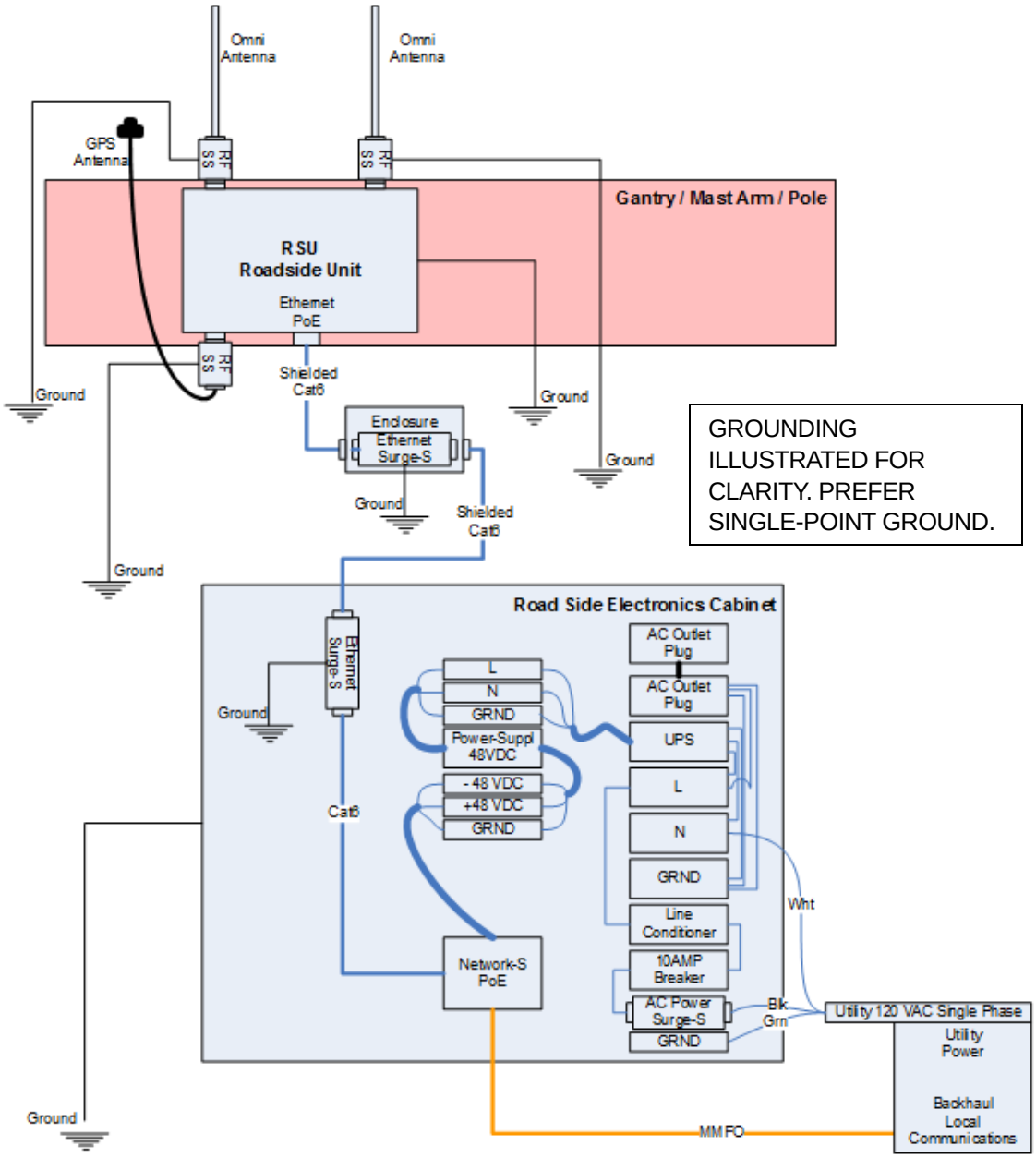

Figure 2-3. Diagram. Configuration for a Roadside Unit Mounted on a Mast Arm.

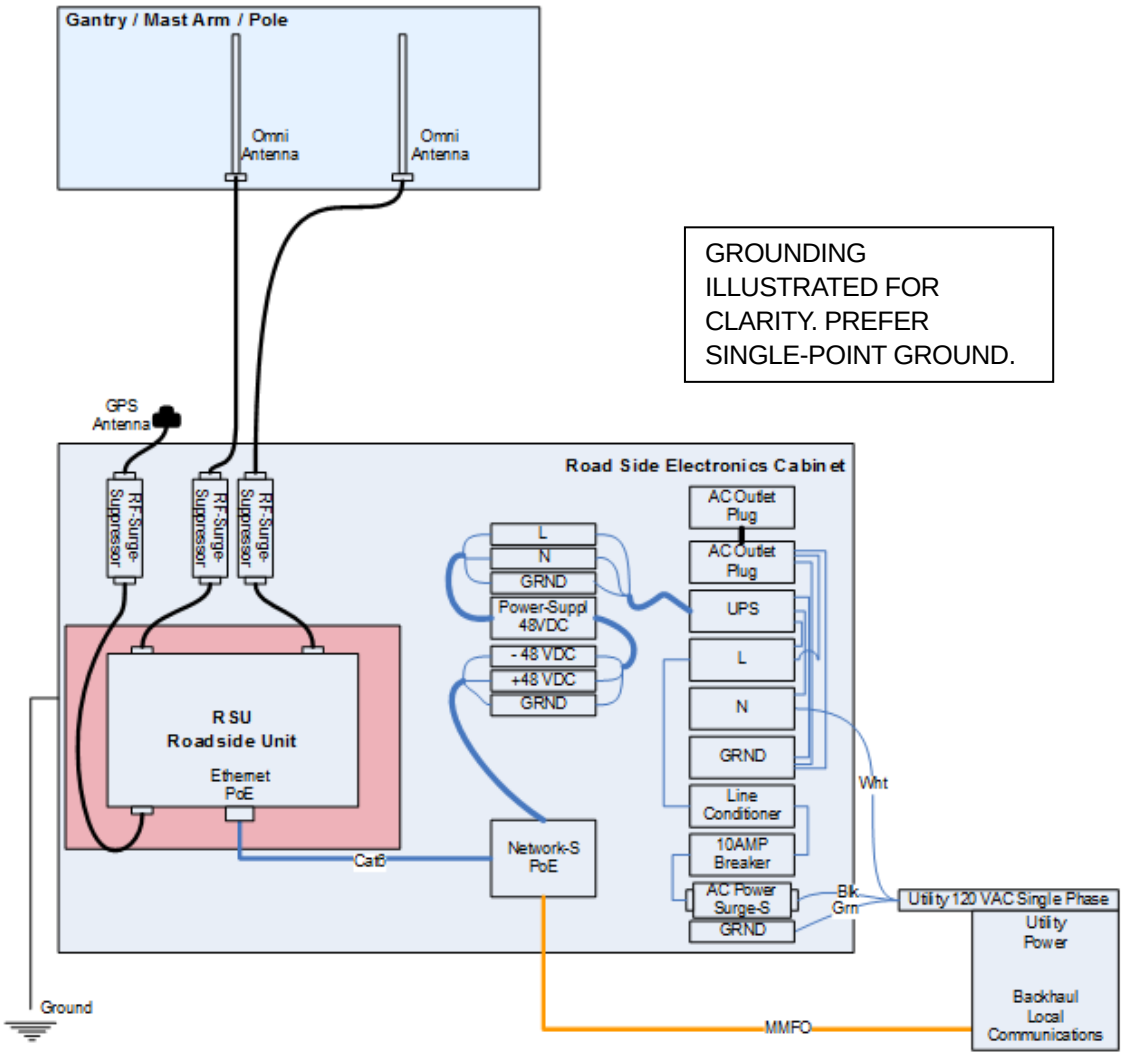

Figure 2-4. Diagram Configuration for a Roadside Unit Installed Inside a Roadside Electronics Cabinet.

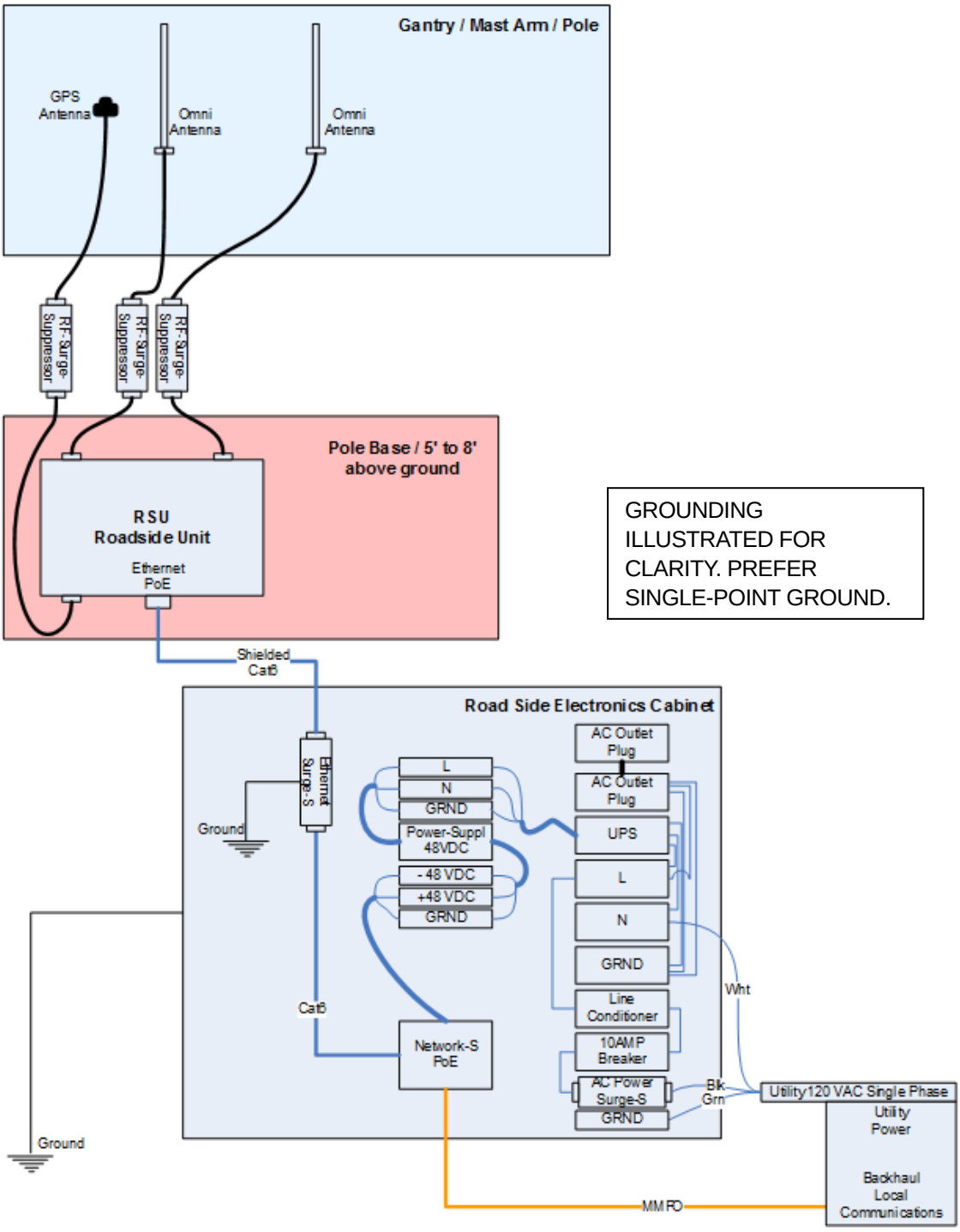

Figure 2-5. Diagram. Configuration for a Roadside Unit Mounted on a Roadside Pole Base, 5–8 Feet Off the Ground.

Furthermore, deployment locations that require the installation of multiple RSUs will be referred to as an "RSU System," that function as a single unit and are connect to the supporting infrastructure through a single physical interface.

Basic Functionality

Figure 2-6 is a basic Context Diagram highlighting Inputs and Outputs, Enablers and Controls, and Activities of an RSU.

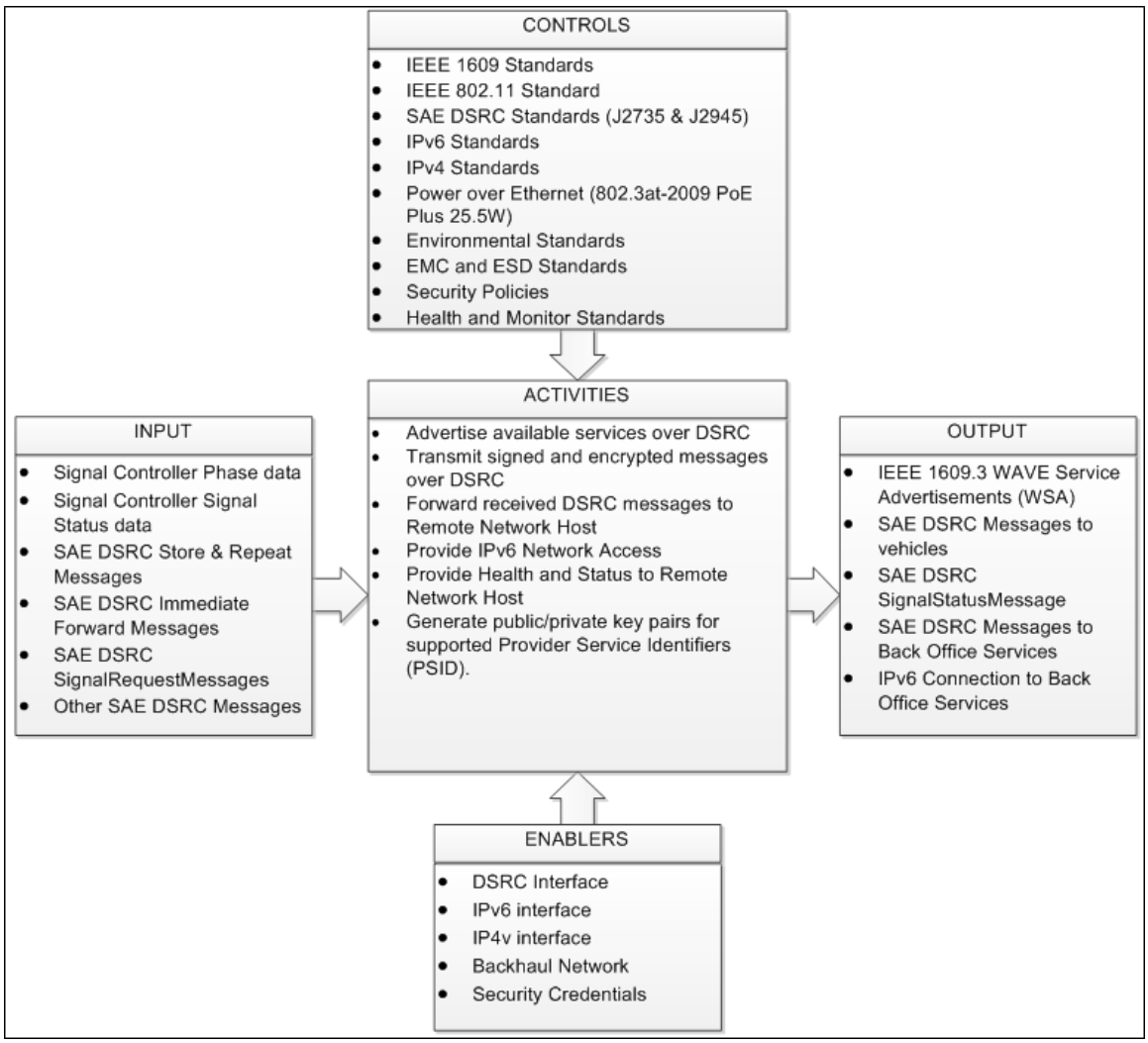

Figure 2-6. Diagram. Context Diagram for a Roadside Unit.

An RSU performs two core functions in a connected vehicle system:

- Provide IPv6 access to remote network hosts.
- Broadcast and receive messages as defined in SAE J2735.

IPv6 Access

The RSU provides DSRC-equipped mobile devices with access to Back Office services by way of IPv6. This allows devices to take advantage of services such as the USDOT Situation Data Clearinghouse, Situation Data Warehouse, and Security Credential Management System (SCMS) as well as other public and private network services. In the case of the Situation Data Clearinghouse and

Situation Data Warehouse, data related to traffic conditions (speed, volume, etc.) are sent from a vehicle over DSRC through an RSU to the Situation Data Clearinghouse and Situation Data Warehouse utilizing the RSUs backhaul connection. In the case of the SCMS, a vehicle is able to send requests for updated certificates through the RSU to the SCMS and receive the updated certificates after the request is processed.

Certificates may take a significant time to process, so it is feasible that a vehicle device would make a request for certificates while it is within range of one RSU and receive them when in range of another RSU.

Application Layer Protocol Data Units (PDU)

The RSU transmits Application Layer Protocol Data Units (PDU) (messages) formatted in accordance with SAE J2735 using one of two mechanisms:

- Store and Repeat
- Immediate Forward

Store and Repeat messages are downloaded from a back office service and stored on the RSU. Transmit Instructions are included with each message that defines how often the message should be transmitted, when the message should start being transmitted, when the message should stop being transmitted, the channel that should be used for the transmission, the Provider Service Identifier (PSID) the message is associated with, and whether the message should be signed and/or encrypted. These transmission instructions should be extracted from the stored message and written to the appropriate Simple Network Management Protocol (SNMPv3) Object Identifier (OID). Once the message expires, it should be removed from RSU storage and the associated SNMPv3 OID should be cleared.

The RSU transmits Immediate Forward messages as they are sent to the RSU. Transmission instructions accompany messages, including the channel that should be used for the transmission, the PSID the message is associated with, and whether the message should be signed and/or encrypted. These transmission instructions should be extracted from the Immediate Forward message and written to the appropriate SNMPv3 OID. The associated SNMPv3 OID should be cleared once the Immediate Forward messages cease.

To support these two functions the RSU must obtain and manage digital certificates to sign and encrypt the messages. The RSU will have the ability to sign every nth message where n is a configurable number programmed into the RSU.

The RSU also receives messages broadcast by a DSRC-equipped mobile device and forwards them to a remote host. Messages are forwarded based on the PSID. The PSID of the message to be forwarded, the IP address and port number of the remote host, the transport protocol to use, the Receive Signal Strength, the interval at which to forward, and the time period during which to forward are all configurable. The configurable parameters are stored in an appropriate SNMPv3 OID. This allows for capabilities such as traffic monitoring, health and status reporting, and certificate requests.

Document Overview

The following section explains how the requirements nomenclature is constructed and numbered.

Each requirement contains a unique ID for traceability and configuration management. For the USDOT Roadside Unit, each requirement will begin with "USDOT_RSU-Req" which is "USDOT Roadside Unit-Requirement-XvY" were "x" is the unique ID and "Y" is the version number.

The columns in the requirements tables throughout this document have the following definitions:

ReqID: a unique identifier providing a reference to a specific requirement. The ID is comprised on a system name, requirement number, and a version number.

Example: USDOT Roadside Unit requirement 1 version 0 would be **USDOT_RSU-*Req-1v0***

The IDs are generated by IBM Rational DOORS (the Requirements Management tool used for this document) in the order in which they were entered into the tool. Requirements may not be listed in numerical order

Description-Statement of the business function or conditions the system must meet

Reference- Additional requirement(s), documents, standards, etc. relating to the function or condition the system must meet

Verification Method- The method utilized to verify the function or condition. The four methods utilized to verify the function or conditions the system must meet are as follows:

1. **Inspection:** Nondestructive examination of the system using one or more of the five senses (visual, auditory, smell, tactile, taste). This may include simple physical manipulation and measurements.
2. **Demonstration:** Manipulation of the system as it is intended to be used to verify that the results are as planned or expected.
3. **Test:** Verification of the system using a controlled and predefined series of inputs, data, or stimuli to ensure that the system will produce a very specific and predefined output as specified by the requirements.
4. **Analysis:** Verification of the system using models, calculations and testing equipment. Analysis allows someone to make predictive statements about the typical performance of a product or system based on the confirmed test results of a sample set or by combining the outcome of individual tests to conclude something new about the product or system. It is often used to predict the breaking point or failure of a product or system by using nondestructive tests to extrapolate the failure point.
5. **Documentation:** Review of documentation including, but not limited to a Data Sheet, Users Guide, Operations Manual, etc.

The requirements contained in this document shall be verified by accredited test facilities. The type of facility charged with verification of each requirement will depend on whether the requirement specifies a physical or operational criterion.

Physical criteria include all technical, mechanical, power, and environmental requirements for the device and shall be evaluated by test facilities that are recognized as having the relevant expertise as defined by the standard or specification referenced in the individual requirements.

Operational criteria include all functional, performance and security requirements for the device and shall be evaluated by facilities compliant with the USDOT requirements. These requirements will be included in the final version of this document.

Conformance

Requirements listed in this document use the following terminology:

- SHALL: indicates that the definition is an absolute requirement of the specification.
- SHALL NOT: Indicates that the definition is an absolute prohibition of the specification.
- SHOULD (RECOMMENDED): Indicates that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- SHOULD NOT (NOT RECOMMENDED): Indicates that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
- MAY (OPTIONAL): Indicates that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option SHALL be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option SHALL be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

References

This section contains all referenced documents, and their appropriate versions, required to meet the specifications contained in this document. The dates referenced in this table should be used as the earliest version of the references applicable to this specification; subsequent updates to the references listed below are applicable to the specifications contained in this document. Hyperlinks to the publications, or websites that offer purchase/subscription access to the publications, have been included below. In some cases, where subscription or purchase is required, temporary access may be available upon request through the Turner-Fairbank Highway Research Center library.

Table 2-2. Useful References.

Reference Number	Document Name
1.	USDOT DSRC Roadside Unit (RSU) Specification version 4.0 (2014)
2.	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 802.11-2012, or later)
3.	IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture (IEEE 1609.0-2013, or later)
4.	Standard for Wireless Access in Vehicular Environments (WAVE) – Security Services for Applications and Management Messages (IEEE 1609.2-2016 as modified by guidance notes, or later)
5.	Standard for Wireless Access in Vehicular Environments (WAVE) – Networking Services (IEEE 1609.3-2016, or later)
6.	Standard for Wireless Access in Vehicular Environments (WAVE) – Multi-Channel Operations (IEEE 1609.4-2016, or later)
7.	Standard for Wireless Access in Vehicular Environments (WAVE) – Identifier Allocations (IEEE 1609.12-2016, or later)
8.	Dedicated Short Range Communications (DSRC) Message Set Dictionary (SAE J2735, 2016 or later)
9.	Standard for Power over Ethernet (IEEE 802.3at, 2009)
10.	NEMA Standard for Traffic Controller Assemblies with NTCIP Requirements (NEMA TS 2-2003 v02.06)
11.	Military Standard for Environmental Engineering Considerations and Laboratory Tests (MIL-ST-810G)
12.	AASHTO Standard Specifications for Structural Supports of Highway Signs, Luminaries, and Traffic Signals (AASHTO LTS-5-I2)
13.	International Electrotechnical Commission Standard for Environmental Testing (IEC-60068-2-6)
14.	International Electrotechnical Commission Standard for Classification of Environmental Conditions (IEC-60721-3-4)
15.	Standard for Electromagnetic Compatibility Measurement Procedures and Limits for Components of Vehicles, Boats, and Machines (SAEJ1113, 2013)
16.	International Electrotechnical Commission Standard for Electromagnetic Compatibility (IEC EN61000-3-2)
17.	NEMA Standard for Enclosures for Electrical Equipment (NEMA 250-2008)
18.	DARPA Internet Program Protocol Specification version 4 (IPv4) (as specified in IETF RFC 790 and IETF RFC 791)
19.	DARPA Internet Program Protocol Specification version 6 (IPv6) (as specified in IETF RFC 2460 and IETF RFC 4291)
20.	On-Board System Requirements for V2V Safety Communications (SAE J2945/1, 2016 or later)
21.	USDOT Security Credential Management System Proof–of–Concept Implementation EE Requirements and Specifications Supporting SCMS Software Release 1.1 or later
22.	Federal Communications Commission (FCC) Code of Federal Regulations Title 47,

Reference Number	Document Name
	Parts 0, 1, 2, 15, 90, and 95
23.	USDOT DTFH61-12-D-00020 DSRC RSU v4.0 Test Plan
24.	Federal Information Processing Standards (FIPS) Publication 140-2 – Security Requirements for Cryptographic Modules
25.	Transport Layer Security (TLS) Protocol Version 1.2 (IETF RFC 5246, August 2008)
26.	Secure Shell (SSH) Version 2 (as specified in IETF RFC 4251, IETF RFC 4252, IETF RFC 4253, and IETF RFC 4254)
27.	Simple Network Management Protocol Version 3 (SNMPv3) (as specified in IETF RFC 3411, IETF RFC 3412, IETF RFC 3413, IETF RFC 3414, IETF RFC 3415, IETF RFC 3416, IETF RFC 3417, and IETF RFC 3418)
28.	Navstar GPS Space Segment/Navigation User Interfaces Interface Specification (IS-GPS-200H)

Chapter 3. System Requirements

This section contains the system requirements to meet USDOT specifications for a DSRC Roadside Unit. These function-based specifications are not intended to prescribe any specific method of implementation, but rather to describe the minimum device functionality. The specifications are broken down into the following categories:

- Power
- Environmental
- Physical
- Functional
- Behavioral
- Performance
- Interface.

Any external agency, including state/local transportation agencies, universities or other research organizations, may specify additional requirements necessary to meet the objectives of a specific project, application, or deployment. Furthermore, individual vendors may choose to include additional functionality so long as it does not interfere with these minimum requirements.

Table 3-1. Operating System Requirements.

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_343-v003	Operating System: The roadside unit operating system SHALL consist of a distribution mechanism in which the developer or developer community could proactively provide updates and patches to remediate vulnerabilities.		

Power Requirements

This section defines the power requirements that will be expected of a compliant roadside unit.

Table 3-2. Power Requirements.

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_278-v001	Operating Voltage: The roadside unit SHALL have a nominal operating voltage between 37 and 57 V DC, compliant with IEEE 802.3at.	IEEE 802.3at	Test: A "Pass" indication contained in a Test Report from an accredited test facility
USDOT_RSU-Req_310-v001	Power over Ethernet: The roadside unit SHALL support inbound power through a single, designated Ethernet port by Power-over-Ethernet (PoE) in compliance with 802.3at.	IEEE 802.3at	Test: A "Pass" indication contained in a Test Report from an accredited test facility
USDOT_RSU-Req_362-v002	Power Injector: any accompanying power injector SHALL be compliant with 802.3at.	IEEE 802.3at	Test: A "Pass" indication contained in a Test Report from an accredited test facility

Environmental Requirements

The roadside unit and all constituent equipment shall be designed to operate within the constraints of the environmental requirements described in this section.

Table 3-3. Environmental Requirements.

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_312-v001	Ambient Temperature RSU: The roadside unit SHALL function as intended within the temperature range of -34 degrees C (-30 degrees F) to +74 degrees C (+165 degrees F).	NEMA TS 2-2003 v02.06	Test: A "Pass" indication contained in a Test Report from an accredited test facility
USDOT_RSU-Req_546-v002	Ambient Temperature Power Injector: any accompanying Power Injector unit SHALL function as intended within the temperature range of -34 degrees C (-30 degrees F) to +74 degrees C (+165 degrees F).	NEMA TS 2-2003 v02.06	Test: A "Pass" indication contained in a Test Report from an accredited test facility
USDOT_RSU-Req_313-v001	Ambient Temperature Rate of Change RSU: The roadside unit 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.	NEMA TS 2-2003 v02.06	Test: A "Pass" indication contained in a Test Report from an accredited test facility

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_547-v002	Ambient Temperature Rate of Change Power Injector: Any accompanying Power Injector unit 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.	NEMA TS 2-2003 v02.06	Test: A "Pass" indication contained in a Test Report from an accredited test facility
USDOT_RSU-Req_314-v001	Storage Temperature RSU: The roadside unit SHALL function as intended after storage at a temperature range of -45 degrees C (-50 degrees F) to +85 degrees C (+185 degrees F).	NEMA TS 2-2003 v02.06	Test: A "Pass" indication contained in a Test Report from an accredited test facility
USDOT_RSU-Req_548-v002	Storage Temperature Power Injector: Any accompanying Power Injector unit SHALL function as intended after storage at a temperature range of -45 degrees C (-50 degrees F) to +85 degrees C (+185 degrees F).	NEMA TS 2-2003 v02.06	Test: A "Pass" indication contained in a Test Report from an accredited test facility
USDOT_RSU-Req_315-v001	Humidity – Average Temperatures RSU: The roadside unit SHALL be capable of continuous operation 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).	NEMA TS 2-2003 v02.06	Test: A "Pass" indication contained in a Test Report from an accredited test facility
USDOT_RSU-Req_549-v002	Humidity – Average Temperatures Power Injector: Any accompanying Power Injector unit SHALL be capable of continuous operation 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).	NEMA TS 2-2003 v02.06	Test: A "Pass" indication contained in a Test Report from an accredited test facility
USDOT_RSU-Req_316-v001	Rain: The roadside unit SHALL pass the rain test with a rainfall rate of 1.7 mm/min (4in/hour), wind speed of 18 m/sec (40 mph) and 30 minutes on each surface of the device as called out in MIL-STD-810 G method 506.5 Procedure 1.	MIL-STD-810 G method 506.5 Procedure 1	Test: A "Pass" indication contained in a Test Report from an accredited test facility

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_317-v001	Salt Fog: The roadside unit SHALL pass the salt fog test with 5% saline exposure for 2 cycles x 48 hours (24 hours wet/24 hours dry) as called out in MIL-STD-810 G method 509.5.	MIL-STD-810 G method 509.5	Test: A "Pass" indication contained in a Test Report from an accredited test facility
USDOT_RSU-Req_318-v001	Wind: The roadside unit mounting bracket SHALL be able to withstand winds up to 150 miles per hour per AASHTO Special Wind Regions Specification.B19	AASHTO Standard Specifications for Structural Supports for Highway Signs, Luminaires, and Traffic Signals, version 6 - Section 3.8.	Test: A "Pass" indication contained in a Test Report from an accredited test facility
USDOT_RSU-Req_319-v002	Operating Shock and Vibration RSU: The roadside unit SHALL comply with the United States Military Standard MIL-STD-810G.	MIL-STD-810G (Ground Transportation Random Vibration and Mechanical Shock) Methods 514.6E-1 and 516.6	Test: A "Pass" indication contained in a Test Report from an accredited test facility
USDOT_RSU-Req_550-v003	Operating Shock and Vibration Power Injector: Any accompanying Power Injector unit SHALL comply with the United States Military Standard MIL-STD-810G.	MIL-STD-810G (Ground Transportation Random Vibration and Mechanical Shock) Methods 514.6E-1 and 516.6	Test: A "Pass" indication contained in a Test Report from an accredited test facility
USDOT_RSU-Req_320-v001	Shock and Vibration Testing RSU: The roadside unit SHALL pass environmental testing conducted in accordance with the procedures specified in IEC-60068 and IEC-60721.	IEC-60068 (Environmental Testing) Section 2-6 Procedures B1, C1 IEC-60721 (Classification of Environmental Conditions) Section 3-4 Class 4M3	Test: A "Pass" indication contained in a Test Report from an accredited test facility

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_551-v002	Shock and Vibration Testing Power Injector: Any accompanying Power Injector unit SHALL pass environmental testing conducted in accordance with the procedures specified in IEC-60068 and IEC-60721.	IEC-60068 (Environmental Testing) Section 2-6 Procedures B1, C1 IEC-60721 (Classification of Environmental Conditions) Section 3-4 Class 4M4	Test: A "Pass" indication contained in a Test Report from an accredited test facility
USDOT_RSU-Req_439-v001	Transportation Shock and Vibration (RSU packaged for shipment): The roadside unit SHALL comply with the United States Military Standard MIL-STD-810G, Test Method 514.6, Procedure I, Category 4. (Heavy truck profile) for packaging and shipping. Note: Intended to provide reasonable assurance that materiel can withstand transportation and handling including field installation, removal, and repair.	MIL-STD-810G, Test Method 514.6, Procedure I, Category 4. (Heavy truck profile)	Test: A "Pass" indication contained in a Test Report from an accredited test facility
USDOT_RSU-Req_321-v001	Electrical Emissions Susceptibility RSU: The roadside unit SHALL be immune to radio frequency (RF)/Electromagnetic Interference (EMI) per SAE J1113.	SAE J1113	Test: A "Pass" indication contained in a Test Report from an accredited test facility
USDOT_RSU-Req_552-v002	Electrical Emissions Susceptibility Power Injector: Any accompanying Power Injector unit SHALL be immune to radio frequency (RF)/Electromagnetic Interference (EMI) per SAE J1113.	SAE J1113	Test: A "Pass" indication contained in a Test Report from an accredited test facility
USDOT_RSU-Req_322-v002	Electrostatic Discharge RSU: The roadside unit SHALL be able to withstand electrostatic discharges from the air up to +/-15kiloVolts (kV) and electrostatic discharges on contact up to +/-8 kiloVolts (kV), in compliance with IEC EN61000-4-2.	IEC EN61000-4-2	Test: A "Pass" indication contained in a Test Report from an accredited test facility

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_553-v003	Electrostatic Discharge Power Injector: Any accompanying Power Injector unit SHALL be able to withstand electrostatic discharges from the air up to +/-15kiloVolts (kV) and electrostatic discharges on contact up to +/-8 kiloVolts (kV), in compliance with IEC EN61000-4-2.	IEC EN61000-4-2	Test: A "Pass" indication contained in a Test Report from an accredited test facility

Physical Requirements

This section contains the physical specifications that a compliant roadside unit will be expected to meet.

Table 3-4. Physical Requirements

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_324-v001	Weight: The weight of the roadside unit, excluding antennas, mounting hardware and Power-over-Ethernet (PoE) Power Injector, SHALL NOT exceed fifteen (15) pounds		Inspection: weighed using a calibrated scale
USDOT_RSU-Req_325-v001	Enclosure: The roadside unit SHALL be housed in a corrosion-resistant enclosure that is compliant with the NEMA4X (IP66) rating.	NEMA 250-2008	Test: A "Pass" indication contained in a Test Report from an accredited test facility
USDOT_RSU-Req_328-v001	Power over Ethernet Connector: The external Power-over-Ethernet (PoE) connector SHALL be compliant with the Outdoor IP66 rating.	NEMA 250-2008 IEEE 802.3at	Test: A "Pass" indication contained in a Test Report from an accredited test facility
USDOT_RSU-Req_329-v001	Mounting: The roadside unit SHALL support installation on a shelf, wall, or pole (horizontal or vertical).		Inspection
USDOT_RSU-Req_331-v001	Power Indication: The roadside unit SHALL include an LED to indicate the power status of the device in accordance with the following protocol: Off - No Power Solid Green - Device is powered on		Demonstration: verify the status and color of the LED with the device powered off and powered on

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_359-v001	Status Indication: The roadside unit SHALL include an LED to indicate the operational status of the device in accordance with the following protocol: Off - No Power Blinking Green - Device Start-Up Solid Green - Device Operational Amber - Firmware Update In Progress Red-Fault		Inspection:

Functional Requirements

This section contains the specifications for all functions that a roadside unit will be expected to perform. SNMPv3 is expected to be used for all device configurations.

Table 3-5. Functional Requirements.

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_361-v002	RSU Set: At installation locations that require multiple roadside units to provide the required DSRC coverage, all RSUs SHALL be configured to operate as a single functional unit.		Test:
USDOT_RSU-Req_576-v001	RSU Set Master: 1 roadside unit in the RSU Set SHALL be configured as the Set "Master" which will be the basis for the configuration of the other RSUs in the Set.		Test:
USDOT_RSU-Req_577-v001	RSU Set Configuration: All non-Master RSUs in the RSU Set SHALL be automatically configured based on the configuration of the Set "Master" RSU		Test:
USDOT_RSU-Req_580-v002	RSU Set Backhaul: If the RSU Set has a backhaul connection, all data between the Back Office and the RSU Set SHALL route through a single device connecting the RSU Set Master to the other roadside units in the backhaul.		Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_437-v005	DSRC Message Forwarding: The roadside unit SHALL forward WSMP messages received on any DSRC interface, containing a specified PSID, to a specified network host, as configured in SNMPv3 MIB OID 1.0.15628.4.1.7. Note: The WSMP Message Forwarding SNMPv3 MIB Object contains the following information: -PSID -Dest_IP Address -Dest_Port -TransPort_Protocol -RSSI -MsgForwardInterval (RSU forwards every nth message received) -DeliveryStart -DeliveryStop See the SNMPv3 MIB OID 1.0.15628.4.1.7 in **Appendix B** for more information		Test:
USDOT_RSU-Req_438-v004	GPS Output: The roadside unit SHALL send the GPGGA NMEA String to a specified UDP port at a specified rate, upon acquisition of 3 or more Satellites, as configured in SNMPv3 MIB OID 1.0.15628.4.1.8, which contains the following data. -Destination IP Address -port (default is 5115) -sample period (default is 1 second, with a valid range of 1-18000 seconds, in increments of 1 second) See the SNMPv3 MIB OID 1.0.15628.4.1.8 in Appendix B for more information	Req_363	Test:
USDOT_RSU-Req_513-v003	System Time: The roadside unit SHALL maintain a system clock based on timing information from a local positioning system that manages leap second corrections in accordance with	Req_363, IS-GPS-200H Sections 3.3.4, 20.3.3.5.2.4, and 30.3.3.6.2	Test:

ReqID	Description	Reference	Verification Method
	IS-GPS-200H. Note: GPS is intended to serve as the primary time source and the NTP server is intended to be available as a secondary, backup time source in the event that the RSU loses GPS.		
USDOT_RSU-Req_514-v002	System Time Standard: The roadside unit SHALL conform to the Universal Time, Coordinated (UTC) standard with epoch 1 January 1970 00:00:00.	Req_363	Test:
USDOT_RSU-Req_618-v002	The roadside unit SHALL notify a remote host via SNMPv3: • if a time source input has been lost for a configurable period of time or has failed after a configurable number of query attempts (note: the time source itself shall also be indicated) (OID 1.0.15628.4.1.100.0.7) • if the value of an internal clock drift (skew rate) has exceeded a configurable tolerance (OID 1.0.15628.4.1.100.0.8) • if the deviation between two or more time sources has exceeded a configurable threshold (OID 1.0.15628.4.1.100.0.9)		Test:

Positioning

Table 3-6. Positioning Requirements

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_510-v002	Position Determination: The roadside unit SHALL utilize a local subsystem to determine its position on the surface of the earth using a sample rate of 1 Hz or better	Req_363	Test:
USDOT_RSU-Req_511-v001	Positioning Failure Log Entry: The roadside unit SHALL write a CRITICAL entry to the System Log if it is not able to acquire a minimum of 3 Satellites within 20 seconds after entering the "Operate" state		Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_512-v002	Positioning Corrections: The roadside unit SHALL utilize WAAS corrections, when available		Test:
USDOT_RSU-Req_602-v001	GPS Reference: The roadside unit SHALL store a reference set of GPS coordinates for itself		Test:
USDOT_RSU-Req_613-v002	The roadside unit SHOULD evaluate GPS sub-frame data to indicate the legitimacy of the GPS data frame source		Test:
USDOT_RSU-Req_614-v002	The roadside unit SHALL notify a remote host via SNMPv3: • if its GPS position deviates from the stored reference by more than a configurable radius (OID 1.0.15628.4.1.100.0.11) • if a suspicious GPS signal is detected (OID 1.0.15628.4.1.100.0.10) • of its current NMEA GPGGA string at a configurable interval (OID 1.0.15628.4.1.100.0.12)		Test:

System Log Files

This section contains requirements related to the RSUs operating system log (syslog) files. The RSU is expected to generate system log file entries at the appropriate priority level depending on the system event. Typical Linux operating system Log files contain the following priority levels:

- EMERGENCY (Level 1) – The application has completely crashed and is no longer functioning. Normally, this will generate a message on the console as well as all root terminals. This is the most serious error possible. This should not normally be used for applications outside of the system level (file systems, kernel, etc.). This usually means the entire system has crashed.
- ALERT (Level 2) – The application is unstable and a crash is imminent. This will generate a message on the console and on root terminals. This should not normally be used for applications outside of the system level (file systems, kernel, etc.).
- CRITICAL (Level 3) – A serious error occurred during application execution. Someone (systems administrators and/or developers) should be notified and should take action to correct the issue.
- ERROR (Level 4) – An error occurred that should be logged, however it is not critical. The error may be transient by nature, but it should be logged to help debug future problems via error message trending. For example, if a connection to a remote server failed, but it will be retried automatically and is fairly self-healing, it is not critical. But if it fails every night at 2AM, you can look through the logs to find the trend.

- WARNING (Level 5) – The application encountered a situation that it was not expecting, but it can continue. The application should log the unexpected condition and continue on.
- NOTICE (Level 6) – The application has detected a situation that it was aware of, it can continue, but the condition is possibly incorrect.
- INFO (Level 7) – For completely informational purposes, the application is simply logging what it is doing. This is useful when trying to find out where an error message is occurring during code execution.
- DEBUG (Level 8) – Detailed error messages describing the exact state of internal variables that may be helpful when debugging problems.

Table 3-7. System Logging Requirements.

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_500-v001	System Log File: The roadside unit SHALL log system events to a standard operating system Log (Syslog) File		Test:
USDOT_RSU-Req_501-v001	System Log Event Priorities: The Priority Level of events that are recorded in the roadside unit System Log file SHALL consist of all priorities available for the operating system		Test:
USDOT_RSU-Req_503-v001	System Log Default Event Priority: The roadside unit SHALL write an entry in the System Log file for INFO events and above, by default		Test:
USDOT_RSU-Req_502-v001	System Log Event Priority Configuration: The Priority Level of events that are recorded in the roadside unit System Log file SHALL be configurable by authorized users		Test:
USDOT_RSU-Req_504-v002	System Log Time Period-Close: The roadside unit SHALL close open System Log files once per week at a configurable time		Test:
USDOT_RSU-Req_505-v002	System Log Time Period-Open: Upon closing a System Log file, the roadside unit SHALL open a new System Log file.		Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_506-v003	System Log File Storage: At a configurable time, the roadside unit SHALL delete system log files that are older than a configurable age (i.e. the length of time since the file was closed). See the SNMPv3 MIB OID 1.0.15628.4.1.18 in Appendix B for more information		Test:
USDOT_RSU-Req_559-v001	System Log File Access: The roadside unit SHALL allow authorized users to view System Log Files stored in the System Log File directory on the device through an Ethernet interface.		Test:
USDOT_RSU-Req_450-v001	Network Host Connection State Change: The roadside unit SHALL write a WARNING entry to the System Log File when a non-DSRC network host connection changes state. The entry will contain the following data: -Date and Time -interface -new state (connected, not connected)		Test:

Interface Log Files

The RSU will provide operators the ability to capture packets transmitted and received on any enabled communication interface for troubleshooting purposes. Interface logs are not intended for long term data capturing.

Table 3-8. Interface Logging Requirements.

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_516-v001	Interface Log File: The roadside unit SHALL have the ability to log all transmitted and received packets across all enabled communication interfaces, while in the "Operate" State.		Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_542-v002	Interface Log File Default Configurations: All Interface Log File configurations contained in SNMPv3 MIB OID 1.0.15628.4.1.9 SHALL have the following default values: -generate=off -Max file size=20MB -Max collection time=24 hr. See the SNMPv3 MIB 1.0.15628.4.1.9 in Appendix B for more information		Test:
USDOT_RSU-Req_539-v003	Interface Log File Begin Generation: An Interface Log File SHALL be generated for a roadside unit communication interface upon setting the “generate” flag in SNMPv3 MIB OID 1.0.15628.4.1.9 for that interface to "on.” Note: when set to "on" both transmitted and received packets are logged See the SNMPv3 MIB 1.0.15628.4.1.9 in Appendix B for more information		Test:
USDOT_RSU-Req_560-v002	Interface Log File Stop Generation: An Interface Log File SHALL stop being generated for a roadside unit communication interface upon setting the “generate” flag in SNMPv3 MIB OID 1.0.15628.4.1.9 for that interface to "off.” See the SNMPv3 MIB 1.0.15628.4.1.9 in Appendix B for more information		Test:
USDOT_RSU-Req_518-v003	Interface Log File-Separation by each direction of an Interface: A separate and independent Interface log file SHALL be generated for each direction (transmit and receive) of a roadside unit communication interface when the SNMPv3 MIB OIB 1.0.15628.4.1.9 for that interface is set to "on.” See the SNMPv3 MIB 1.0.15628.4.1.9 in Appendix B for more information		Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_541-v002	Interface Log File format: Each Interface Log File SHALL be generated in the industry standard packet capture (pcap) format and contain the following data: -Date and Time (in UTC, when the packet was logged) -RSSI (for Packets Received over DSRC) -TxPower (for Packets Transmitted over DSRC) -packet (complete transmitted or received packet)		Test:
USDOT_RSU-Req_521-v003	Interface Log File Close-Max file size: The roadside unit SHALL close an active Interface Log File upon reaching the configured "Max file size" in SNMPv3 MIB OID 1.0.15628.4.1.9. See the SNMPv3 MIB 1.0.15628.4.1.9 in Appendix B for more information		Test:
USDOT_RSU-Req_522-v001	Interface Log File Close-transition to Standby: The roadside unit SHALL close all active Interface Log Files when transitioning to "standby" state.		Test:
USDOT_RSU-Req_543-v003	Interface Log File Close-Time Limit: The roadside unit SHALL close an active Interface Log File upon reaching the configured "Max collection time" in SNMPv3 MIB OID 1.0.15628.4.1.9. See the SNMPv3 MIB 1.0.15628.4.1.9 in Appendix B for more information		Test:
USDOT_RSU-Req_523-v003	Interface Log File Generation-Max file size: The roadside unit SHALL generate a new Interface Log File upon closing a previously active Interface Log File when the configured "Max file size" in SNMPv3 MIB OID 1.0.15628.4.1.9 is reached. See the SNMPv3 MIB 1.0.15628.4.1.9 in Appendix B for more information		Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_524-v004	Interface Log File Name Convention: Each roadside unit Interface Log File SHALL be named according to the following convention: -RSU ID (see MIB OID 1.0.15628.4.1.17) -Interface ID -transmit, receive, or both -date and time (UTC date and time when the file was created		Test:
USDOT_RSU-Req_527-v002	Interface Log File Access: The roadside unit SHALL allow authorized users to view Interface Log Files stored in the Interface Log File directory on the device through an Ethernet interface.		Test:

Message Processing – Store and Repeat-Encoded Payload

The roadside unit will transmit DSRC messages based on Active Message text files loaded on the device. Each text file will contain the transmission instructions and encoded payload for 1 DSRC message and include the following data elements:

- Message Type/Description
- Message PSID
- Message Priority
- Transmission Channel Mode
- Transmission Channel
- Transmission Interval
- Message Delivery (transmission) start time
- Message Delivery (transmission) stop time
- Signature
- Encryption
- Payload.

The file format is contained in Appendix C.

Table 3-9. Store and Repeat Message Requirements (Encoded Payload).

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_468-v001	Store & Repeat Message Start of Transmission: The roadside unit SHALL begin transmitting the payload of an Active Message text file over a DSRC interface, based on the transmission instructions contained in the Active Message text file, on or after the start time specified in the transmission instructions of the Active Message text file for each Active Message text file stored on the unit. Note: Appendix C contains the message format		Test:
USDOT_RSU-Req_470-v001	Store & Repeat Message End of Transmission: The roadside unit SHALL stop transmitting the payload of an Active Message text file as a DSRC message at end time specified in the transmission instructions of the Active Message text file for each Active Message text file stored on the unit.		Test:
USDOT_RSU-Req_452-v002	Store & Repeat Message Storage: The roadside unit SHALL store at least 100 Active Message text files in an Active Message directory.		Test:
USDOT_RSU-Req_453-v003	Store & Repeat Active Message file installation: The roadside unit SHALL allow authorized users to add/remove Active Message text files to/from the Active Message directory through SNMPv3 OID 1.0.15628.4.1.4.x.		Test:
USDOT_RSU-Req_454-v003	Store & Repeat Active Message file removal: The roadside unit SHALL allow authorized users to remove Messages from the Active Message directory through SNMPv3 OID 1.0.15628.4.1.4.		Test:
USDOT_RSU-Req_455-v003	Store & Repeat Active Message review: The roadside unit SHALL allow authorized users to view the contents of Active Messages in the Active Message directory through SNMPv3 OID 1.0.15628.4.1.4.		Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_457-v003	Store & Repeat Active Message Modification: The roadside unit SHALL allow authorized users to modify an Active Message through SNMPv3 OID 1.0.15628.4.1.4.		Test:
USDOT_RSU-Req_459-v001	Store & Repeat Active Message Authorized Access Log Entry: The roadside unit SHALL write an INFO entry to the System Log File for each authorized access to an Active Message text file containing the following data: -Date and Time -File Name (name of the Active Message text file as stored in the Active Message directory) -Successful operation (installation, removal, or modification) -user ID		Test:
USDOT_RSU-Req_469-v001	Store & Repeat Active Message Failed Access Log Entry: The roadside unit SHALL write a WARNING entry to the System Log File for each failed access attempt to an Active Message text file containing the following data: -Date and Time -File Name (name of the Active Message text file as stored in the Active Message directory) -Failed operation (install, remove, modify) -user ID		Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_462-v001	Store & Repeat Active Message Transmission Log Entry: The roadside unit SHALL write a NOTICE entry to the System Log File when an Active Message changes transmission status resulting from a user initiated device shut down, device boot up, message start time or message end time. Each entry will contain the following data: -Date and Time -File Name (name of the Active Message text file as stored in the Active Message directory) -Transmission Status (Start/Stop)		Test:

Message Processing – Store and Repeat-Raw Data Payload

If supported, the roadside unit will transmit DSRC messages based on configuration text files containing raw, un-encoded data, loaded on the device. Each text file will contain the transmission instructions and human readable data elements for 1 DSRC message and include the following data elements:

- Message Type/Description
- Message PSID
- Message Priority
- Transmission Channel Mode
- Transmission Channel
- Transmission Interval
- Message Delivery (transmission) start time
- Message Delivery (transmission) stop time
- Signature
- Encryption
- <list of raw data elements>.

Table 3-10. Store and Repeat Message Requirements (Raw Data Payload).

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_562-v001	Raw Data Text File: The roadside unit MAY store raw data text files for encoding into messages to be transmitted over a DSRC interface Note: This is similar to the Store & Repeat functionality described in Section 3.4.4 with the exception that the file stored on the RSU would contain raw, un-encoded, data to be encoded prior to being transmitted over DSRC. For Example a human readable/configurable Map configuration file		Test:
USDOT_RSU-Req_563-v001	Raw Data Text File Encoding: The roadside unit MAY encode raw data contained in a text file residing on the RSU into messages to be transmitted over a DSRC interface Note: This is similar to the Store & Repeat functionality described in Section 3.4.4 with the exception that the RSU would encode the raw data contained in the stored file into a DSRC Payload of the appropriate format prior to transmitting over DSRC. For Example a human readable/configurable Map configuration file		Test:

Message Processing – Immediate Forward-Encoded Payload

The roadside unit will transmit DSRC messages based on information received from a network host. Each Immediate Forward (IF) message received from a network host will contain the transmission instructions and payload for 1 DSRC message and include the following data elements:

- Message Type/Description
- Message PSID
- Message Priority
- Transmission Channel Mode
- Transmission Channel
- Transmission Interval (set to Null)

- Message Delivery (transmission) start time (set to Null)
- Message Delivery (transmission) stop time (set to Null)
- Signature
- Encryption
- Payload.

Appendix C contains the format of the Immediate Forward Message.

Table 3-11. Immediate Forward Requirements (Encoded Payload)

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_554-v001	Immediate Forward Message Receive: The roadside unit SHALL receive messages for Immediate Forward from network hosts on default UDP port 1516 Note: Appendix C contains the Immediate Forward message format		Test:
USDOT_RSU-Req_471-v003	Immediate Forward Message Transmission: The roadside unit SHALL transmit over a DSRC interface each message payload received from a network host upon receipt of the message and according to the transmission instructions contained in the message header. Note: Appendix C contains the Immediate Forward message format		Test:

Message Processing – Immediate Forward-Raw Data Payload

If supported, the roadside unit will transmit DSRC messages based on raw, un-encoded, data received from a network host. Each data stream will include raw data elements for 1 DSRC message. The following transmission instructions should be applied to each message:

- Message Type/Description
- Message PSID
- Message Priority
- Transmission Channel Mode
- Transmission Channel
- Transmission Interval (set to Null)
- Message Delivery (transmission) start time (set to Null)

- Message Delivery (transmission) stop time (set to Null)
- Signature
- Encryption.

Table 3-12. Immediate Forward Requirements (Raw Data Payload)

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_565-v001	Raw Data Stream: The roadside unit MAY accept raw data over a non-DSRC Interface for encoding into messages to be transmitted over a DSRC interface Note: This is similar to the Immediate Forward functionality described in Section 3.4.6 with the exception that the RSU will receive raw, un-encoded, data from a network host that must be encoded prior to being transmitted over DSRC. For example: raw SPaT data from a Signal Controller		Test
USDOT_RSU-Req_566-v001	Data Stream Message Encoding: The roadside unit MAY encode raw data received on a non-DSRC interface into messages to be transmitted over a DSRC interface Note: This is similar to the Immediate Forward functionality described in Section 3.4.6, with the exception that the RSU will encode the raw data into a DSRC Payload of the appropriate format prior to transmitting over DSRC. For example: raw SPaT data from a Signal Controller.		Test

Security

Table 3-13. Security Requirements.

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_567-v001	Physical Security: The roadside unit SHALL be compliant with Federal Information Processing Standard (FIPS) 140-2 Level 2 Physical Security Requirements	FIPS 140-2	Test:
USDOT_RSU-Req_585-v001	Physical Security: The roadside unit SHOULD be compliant with Federal Information Processing Standard (FIPS) 140-2 Level 3 Physical Security Requirements that require a tamper response mechanism, such as sending off an indicator to the backhaul network.	FIPS 140-2	Test:
USDOT_RSU-Req_344-v002	Authentication: The roadside unit SHALL be protected by a password compliant with either local operator security policies or a policy based on existing standards (e.g., FIPS 140- Level 3 and 4 in Section 4.3.3)	FIPS 140-2 Section 4.3.3	Test:
USDOT_RSU-Req_467-v001	Authentication: The roadside unit SHALL support multiple SNMPv3 users each with an individual password		Test:
USDOT_RSU-Req_345-v001	Authentication: The roadside unit SHOULD support multi-factor authentication.		Test:
USDOT_RSU-Req_632-v002	Authentication: The roadside unit SHOULD enforce multi-factor authentication on all SSH Version 2 sessions, and, if supported, all TLS-based remote access sessions to the roadside unit.	Secure Shell (SSH) Version 2 (as specified in IETF RFC 4251, IETF RFC 4252, IETF RFC 4253, and IETF RFC 4254) Transport Layer Security (TLS) Protocol Version 1.2 (IETF RFC 5246, August 2008)	Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_346-v002	Authentication: The roadside unit SHALL support password recovery for the RSU User Accounts that cannot be violated by physical access alone.		Test:
USDOT_RSU-Req_347-v002	Configuration: The roadside unit configuration files SHOULD enforce digital signatures to prevent unauthorized modifications.	FIPS 186-4	Test:
USDOT_RSU-Req_348-v001	Access Control: The roadside unit SHALL restrict remote network access based on an IP Address Access Control List (ACL) Note: The RSU can only be accessed from the IP Addresses contain in the ACL.		Test:
USDOT_RSU-Req_350-v001	Data Protection: The roadside unit local file system SHOULD be encrypted		Test:
USDOT_RSU-Req_351-v002	Interfaces: Each roadside unit Ethernet interface SHALL be protected by a configurable firewall with a default to be closed.		Test:
USDOT_RSU-Req_440-v002	Access Control: If so equipped, Web-Based access to the roadside unit SHALL only be through Hypertext Transfer Protocol Secure (HTTPS)		Test:
USDOT_RSU-Req_442-v002	Data Protection: the roadside unit SHOULD synchronize its system clock to a Network Time Protocol (NTP) Service in the event that it loses GPS fix.		Test: if available
USDOT_RSU-Req_355-v001	Authentication: If the roadside unit synchronizes it's system clock to a Network Time Protocol (NTP) service, the device SHALL authenticate messages received from the NTP service	Req_442	Test: if available
USDOT_RSU-Req_356-v003	Access Control: The roadside unit SHALL only be accessible through the following network protocols: Secure Shell version 2 (SSHv2) SNMPv3 SCP TLS (HTTPS)		Test: log in attempts will be made using SSHv2

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_583-v001	Configuration: network protocol Secure Shell version 2 SHOULD be configured as follows: Root Login Disable root Use certificate-based authentication, rate-limited (to slow down brute-force attempts) use FIPS 140-2-compliant cryptography	FIPS 140-2	Test:
USDOT_RSU-Req_606-v001	Data Protection: The roadside unit SHALL immediately apply integrity protections to the store-and-repeat message data following SNMP-secured download to the roadside unit.	Section 3.4.4,Section 3.4.5, Req_607	Test:
USDOT_RSU-Req_607-v001	Data Protection: The roadside unit SHALL verify the integrity of the store-and-repeat message data prior to generating and transmitting IEEE 1609.2-secured messages that are derived from the message data.	Section 3.4.4 and Section 3.4.5	Test:
USDOT_RSU-Req_609-v001	Data Protection: The roadside unit SHALL inhibit construction and transmission of an IEEE 1609.2-secured message derived from an integrity-failed store-and-repeat message.	Section 3.4.4 and Section 3.4.5	Test:
USDOT_RSU-Req_615-v001	Notification: The roadside unit SHALL notify a remote host via SNMPv3: if an Active Message fails an Integrity check if a configurable number of consecutive authentication attempts have failed if the signature of a signed DSRC message has failed verification of any access control errors and rejections		Test:
USDOT_RSU-Req_616-v001	Notification: If secure storage is available, the roadside unit SHALL notify a remote host via SNMPv3 if the secure parameters stored in secure storage have failed an Integrity check.	Req_579	Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_617-v001	Notification: If FIPS 140-2 level 3 is implemented, the roadside unit SHALL notify a remote host via SNMPv3 if the enclosure has been tampered with according to FIPS 140-2 Section 4.5 Level 3 tamper indication requirements.	FIPS 140-2 Section 4.5 Level 3	Test:
USDOT_RSU-Req_619-v001	Access Control: The roadside unit SHALL enforce clear associations between roles, services and the distinct authentication and authorizations required to access those services.		Test:
USDOT_RSU-Req_620-v001	Access Control: Access to sensitive services SHALL require an authenticated, authorized role.		Test:
USDOT_RSU-Req_621-v001	Access Control: Access to sensitive data SHALL require an authenticated, authorized role.		Test:
USDOT_RSU-Req_622-v001	Authentication: The roadside unit SHALL be configurable to limit the number of repeated authentication attempts for services requiring authentication.		Test:
USDOT_RSU-Req_623-v002	Authentication: The roadside unit SHOULD utilize certificate pinning to secure all TLS sessions with the SCMS Device Configuration Manager and other SCMS nodes to which it connects.	Transport Layer Security (TLS) Protocol Version 1.2 (IETF RFC 5246 and IETF RFC 7469) with cipher suites pinned to USDOT Security Credential Management System Design: Security Credential Management System Proof–of–Concept Implementation EE Requirements and Specifications Supporting SCMS Software Release 1.1, published May, 2016, or later	Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_625-v001	Authentication: The roadside unit SHALL terminate a TLS session if the server public key certificate signature verification fails during TLS session establishment.	Transport Layer Security (TLS) Protocol Version 1.2 (IETF RFC 5246, August 2008)	Test:
USDOT_RSU-Req_627-v001	Authentication: The roadside unit should verify the IEEE 1609.2 digital signature on all messages previously signed by the TMC or other backhaul services prior to forwarding over the DSRC interface.		Test:
USDOT_RSU-Req_628-v002	Authentication: Services requiring role- or identity-based authentication SHALL meet the authentication requirements of FIPS 140-2, Section 4.3 Level 2 and any supporting FIPS 140-2 implementation guidance.	FIPS 140-2, Section 4.3 Level 2 and Level 3	Test:
USDOT_RSU-Req_629-v001	Authentication: Services requiring authentication SHALL meet the single attempt and multiple attempt authentication strength requirements of FIPS 140-2, Section 4.3.	FIPS 140-2, Section 4.3	Test:
USDOT_RSU-Req_630-v001	Authentication: The roadside unit SHALL require SSH Version 2 or TLS Version 1.2 using mutual (two way) public key credential authentication for all authorized user sessions.	Secure Shell (SSH) Version 2 (as specified in IETF RFC 4251, IETF RFC 4252, IETF RFC 4253, and IETF RFC 4254) Transport Layer Security (TLS) Protocol Version 1.2 (IETF RFC 5246, August 2008)	Test:
USDOT_RSU-Req_631-v001	Authentication: The roadside unit SHALL require HTTPS using mutual (two way) public key credential authentication for all HTTPS connections to the roadside unit.		Test:
USDOT_RSU-Req_635-v001	Configuration: The roadside unit SHALL be configurable regarding the maximum frequency (number per second) or ratio (percentage) of DSRC message digital signatures to verify based on PSID.	Section 3.4.4 and Section 3.4.5	Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_636-v001	Configuration: The roadside unit SHALL be able to be configured whether to accept, drop, or respond to application-specific messages signed with expired certificates.	Section 3.4.4 and Section 3.4.5	Test:
USDOT_RSU-Req_638-v001	Data Protection: The roadside unit SHALL cryptographically protect the integrity of all configuration information provided by the SCMS Device Configuration Manager (DCM).		Test:
USDOT_RSU-Req_639-v002	Data Protection: All cryptographic keys SHALL be established or generated using a FIPS Approved and allowed key generation and key establishment mechanisms.	FIPS 140-2 Annex A and Annex D	Test:
USDOT_RSU-Req_640-v001	Data Protection: All sensitive roadside unit system files and application files SHALL be digitally signed using a digital signature algorithm listed in FIPS 186-4.	FIPS 186-4	Test:
USDOT_RSU-Req_641-v001	Data Protection: The roadside unit SHALL successfully verify the digital signature on all sensitive roadside unit system and application files prior to exposing any services.		Test:
USDOT_RSU-Req_642-v001	Data Protection: The roadside unit SHALL implement a secure mechanism in software to securely store and provide strict access controls to all sensitive security parameters, including: -TLS public and private keys (as used for HTTPS or other TLS tunneling, including with the SCMS) -SSH public and private keys -Passwords -SNMP keys and passphrases -Any sensitive security parameters not stored in a hardware secure storage mechanism	Req_579	Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_643-v001	Data Protection: Software secure storage SHALL: -prevent read-access to all stored security parameters, -maintain integrity of all security parameters, including associations of keys with entities and processes -check the integrity of stored security parameters when accessing -prevent unauthorized modification of security parameters, except by authorized users -prevent unauthorized addition of security parameters, except by authorized users -prevent unauthorized substitution of security parameters, except by authorized users -encrypt all sensitive security parameters when not in use	Req_579	Test:
USDOT_RSU-Req_644-v001	Data Protection: The roadside unit SHALL store passwords in secure storage only after modifying via a one-way cryptographic function.	Req_579	Test:
USDOT_RSU-Req_645-v001	Data Protection: The roadside unit SHALL zeroize all non-factory installed parameters, cryptographic keys, applications, data and configurations when undergoing a factory reset.	Req_568	Test:
USDOT_RSU-Req_646-v001	Data Protection: Upon sudden loss of external power, the roadside unit SHALL undergo a shutdown procedure that preserves file system integrity.		Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_647-v001	Interfaces: The roadside unit SHALL utilize TLS versions and cipher suites consistent with SCMS interface specifications.	USDOT Security Credential Management System Design: Security Credential Management System Proof–of–Concept Implementation EE Requirements and Specifications Supporting SCMS Software Release 1.1, published May, 2016, or later	Test:
USDOT_RSU-Req_648-v001	Interfaces: Services and protocols SHALL be able to be inhibited according to physical interface, source/destination IP address and source/destination ports		Test:
USDOT_RSU-Req_649-v002	Logging: The roadside unit SHALL write the following entries to the System Log File: GPS location and time data on a configurable interval metrics on packet integrity or transmission/reception errors all authentication parameter modifications attempts to perform a service allocated to a role(s) for which the entity is not authenticated authorization failures when a role or identity attempts access services and data requiring authorization input and output protocol violations, including encoding errors and invalid parameters session management failures in each of the session-based network protocols it supports all additions, modifications and removal of secret, public and private	FIPS 186-4	Test:

ReqID	Description	Reference	Verification Method
	cryptographic keys success or failure of digitally signing all sensitive roadside unit system and application files using a digital signature algorithm listed in FIPS 186-4 any expired IEEE 1609.2 public key credentials it has stored any expired X.509 public key credentials it has stored pending expirations of all public key credentials to a configurable warning time value		

USDOT Situation Data Clearinghouse and Warehouse

If supported the roadside unit will deposit Intersection Situation Data into the USDOT Situation Data Clearinghouse and retrieve geographic relevant Traveler information messages from the USDOT Situation Data Warehouse.

Table 3-14. Situation Data Requirements.

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_589-v001	Situation Data Clearinghouse: if transmitting Intersection Safety Awareness messages, the roadside unit SHOULD deposit an Intersection Situation Data (ISD) Protocol Data Unit (PDU) (message) into the USDOT Situation Data Clearinghouse once every 2 seconds. Intersection Situation Data Protocol Data Units are comprised of 1 SAE Signal Phase and Timing Message (SPaT) and 1 SAE Map Message. See the SNMPv3 MIB OID 1.0.15628.4.1.20 in Appendix B for more information	USDOT Connected Vehicle Support Services SEMI_v2.3.0_070616.asn or later	Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_590-v002	Situation Data Warehouse: the roadside unit SHOULD retrieve SAE Traveler Information Messages from the USDOT Situation Data Warehouse that are relevant to the roadside unit's geographic location.	USDOT Connected Vehicle Support Services SEMI_v2.3.0_070616.asn or later	Test:

Behavioral Requirements

This section contains the specifications for the expected behavior of a compliant roadside unit.

Table 3-15. Behavioral Requirements

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_496-v002	Configuration Updates-updateconfig command: The roadside unit SHALL update all configuration parameters upon receiving an "updateconf" command from an authorized user		Test:
USDOT_RSU-Req_497-v002	Configuration Updates-SNMPv3 MIB: The roadside unit SHALL update all configuration parameters upon receiving changes to any writable SNMPv3 MIB objects from an authorized user		Test:
USDOT_RSU-Req_604-v002	Antenna Output Power: the roadside unit transmit output power SHOULD be configurable		Test:

Operational States

Table 3-16. Operational State Requirements

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_475-v002	State Transition - Initial to Standby: The roadside unit SHALL transition from the "Initial" State to the "Standby State" upon power on. Note: Transition from the "initial" state to the "standby" state only happens the first time the device is powered on after manufacturing or after factory reset. The device will only return to the "initial" state if a factory reset is initiated.		Test:
USDOT_RSU-Req_476-v002	State Transition - Operate to Standby: The roadside unit SHALL transition from the "Operate" State to the "Standby" State upon receiving a "standby" command from an authorized user		Test:
USDOT_RSU-Req_479-v002	State Transition - Standby to Operate: The roadside unit SHALL transition from the "Standby" State to the "Operate" state upon receiving a "run" command from an authorized user		Test:
USDOT_RSU-Req_480-v002	State Transition - Current to No Power: The roadside unit SHALL transition from its current State to the "No Power" State upon loss of power or user initiated shut down without corrupting or damaging the file system or files contained on the unit.		Test:
USDOT_RSU-Req_575-v001	State Transition - No Power to Previous State: When power is restored, the roadside unit SHALL transition from the “No Power” state to the State (“Standby” or “Operate”) the roadside unit was in when power was lost.		Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_568-v002	Factory Reset: The roadside unit SHALL support a "Factory Reset" mechanism (command, button, etc.) for authenticated, authorized local users to remove all configuration parameters and operator installed files, returning the device to its original Factory Settings and “Initial” State		Test:

Operational Modes

Table 3-17. Operational Mode Requirements

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_482-v001	Operation Mode-Connected: The roadside unit SHALL operate with full functionality while connected to an operations center. Note: "Connected Mode" implies that the RSU is intended to continuously be connected to an operation center		Test:
USDOT_RSU-Req_484-v001	Operation Mode-"Standalone”: The roadside unit SHALL operate with full functionality while not connected to an operations center, until the device’s security credentials expire.		Test:

Operational Configuration

Table 3-18. Operational Configuration Requirements.

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_435-v001	SNMPv3: roadside unit Configuration, Management, and Status information SHALL be provided through SNMPv3. The RSU Management Information Base (MIB) is contained in Appendix B.	Simple Network Management Protocol Version 3 (SNMPv3) (as specified in IETF RFC 3411, IETF RFC 3412, IETF RFC 3413, IETF RFC 3414, IETF RFC 3415, IETF RFC 3416, IETF RFC 3417, and IETF RFC 3418)	Test:
USDOT_RSU-Req_487-v001	SMNPv3 MIB Configurations: The roadside unit SHALL operate based on parameters contained in the SNMPv3 MIB stored on the device.		Test:
USDOT_RSU-Req_489-v001	SMNPv3 MIB Configuration Default Parameters: The roadside unit SHALL have default values for each configuration parameter in the SNMPv3 MIB.		Test:
USDOT_RSU-Req_498-v001	SMNPv3 MIB Configuration Parameter Valid Range: The value of each SNMPv3 MIB Object SHALL be restricted to a valid range in which the roadside unit will operate.		Test:
USDOT_RSU-Req_490-v001	SNMPv3 MIB Walk: The roadside unit SHALL allow an authorized user to perform a MIB walk on the SNMPv3 MIB to produce a complete list of all supported MIBs and OIDs and the current setting for each Object.		Test:
USDOT_RSU-Req_491-v002	SMNPv3 MIB Parameter Modification: The roadside unit SHALL allow an authorized user to modify the value of any writeable SNMPv3 MIB Object within its valid range.		Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_492-v002	SMNPv3 MIB Modification Validation-System Status Log File entry: The roadside unit SHALL write an INFO entry to the System Status Log File if the value of a writable SNMPv3 MIB Object is modified to an out of range value. The log entry will contain the following data elements: • Date and Time • file name (name of the MIB file) • "MIB Object Value Out-of-Range" • OID (of the Object whose value is out of range) • user ID • attempted value		Test:
USDOT_RSU-Req_499-v001	SMNPv3 MIB Modification Validation-retain current value: The roadside unit SHALL retain the current value for a writable SNMPv3 MIB Object that is modified to an out of range value		Test:
USDOT_RSU-Req_493-v001	SNMPv3 MIB installation: The roadside unit SHALL allow authorized users to copy/move a SNMPv3 MIB from a network host to the SMNPv3 MIB directory on the device through an Ethernet Interface.		Test:
USDOT_RSU-Req_494-v001	SNMPv3 MIB copy: The roadside unit SHALL allow authorized users to copy the SNMPv3 MIB from the SNMPv3 MIB directory to a network host through an Ethernet Interface		Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_495-v002	SNMPv3 MIB Installation Validation-System Status Log File entry: The roadside unit SHALL write a CRITICAL entry in the System Status log file if a SNMPv3 MIB that contains out of range values for a writable Object is copied/moved into the SNMPv3 MIB directory. The log entry will contain the following data elements: • Date and Time • file name (name of the MIB file) • "MIB Object Value Out-of-Range:" • OID (of the Object whose value is out of range) • user ID • offending value		Test:

Health and Status Monitoring

Table 3-19. Health and Status Monitoring Requirements.

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_592-v002	The roadside unit SHALL report over SNMPv3: status of its memory (OID ucdavis.4) status of its CPU load status of its non-volatile storage standard system load average values time elapsed since it entered the "Operate" state time elapsed since it was first powered on last user to log in time the last user logged in source IP address of the last user to log in number of messages	UCD-SNMP-MIB	Test:

ReqID	Description	Reference	Verification Method
	transmitted and received over DSRC, sorted by Alternating or Continuous, SCH or CCH, and Sent or Received number of messages transmitted over DSRC, sorted by PSID		
USDOT_RSU-Req_601-v001	The roadside unit SHOULD report over SNMPv3 its internal temperature		Test:

Performance Requirements

This section contains the specifications for the expected performance of a compliant roadside unit.

Table 3-20. Performance Requirements.

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_340-v001	Mean-Time-Between-Failure (MTBF): The roadside unit SHALL remain operational for an average of 100,000 hours.		Analysis: using MIL-HDBK-217 calculation methods
USDOT_RSU-Req_341-v002	Availability: The roadside unit SHALL meet the operational availability requirements of 99.9%. Note: This does not include scheduled maintenance.		Analysis:

Radio Performance

Table 3-21. Radio Requirements.

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_432-v004	DSRC Radio Receive Range: The roadside unit SHALL receive DSRC messages throughout a range of 1m to 300m, with a maximum Packet Error Rate of 10.0%, in an open field under the following conditions: When receiving on an 802.11 Operating class 17 channel (even 10 MHz Service Channel, numbers 172 through 184). When receiving Part 1 of the SAE J2735 defined Basic Safety Message (BSM) With a BSM transmit rate of 10 Hz With a Data Rate of 6 Mbps With an RSU antenna centerline height of 8 meters With a BSM transmit power of VRPMax, as defined in SAE J2945/1	FCC Title 47, Part 90.377 SAE J2945/1	Test: Measure the Packet Error Rate of received Basic Safety Messages on Service Channel 172 at specified distances from the RSU Antenna

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_433-v003	DSRC Radio Transmission Range: The roadside unit SHALL transmit DSRC messages throughout a range of 1m to 300m, with a maximum Packet Error Rate of 10.0%, in an open field under the following conditions: When transmitting on an 802.11Operating class 17 channel (even 10 MHz Service Channel, numbers 172 through 184). When transmitting Wave Service Advertisements (WSA), as defined in IEEE 1609.3 With a WSA Transmission Rate of 10 Hz With a Data Rate of 6 Mbps With an RSU antenna centerline height of 8 meters With a maximum WSA transmit EIRP Using a Receiver conforming to SAE J2945/1 Section 6.4.2	FCC Title 47, Part 90 SAE J2945/1 Section 6.4.2	Test: Transmit a DSRC message on each of the even 10MHz Service Channel and measure the Packet Error Rate at specified distances from the RSU Antenna

Interface Requirements

This section contains the specifications for the internal and external interfaces of a compliant roadside unit.

Table 3-22. Interface Requirements.

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_363-v001	GPS: The roadside unit SHALL include an integrated GPS receiver (for positioning and UTC time).		Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_364-v003	RSU Set Interface: At installation locations that require multiple roadside units, the “master” roadside unit in the set SHALL be functional as the Ethernet interface between other non-master RSUs and the backhaul communication.		Test:
USDOT_RSU-Req_326-v001	Physical Ethernet Interface: The roadside unit SHALL, at a minimum, include a 1x10/100 Base-T Ethernet (RJ45) port that supports 48V DC and is compliant with 802.3at Power-over-Ethernet (PoE), including IPv4 and IPv6.	IEEE 802.3at	Test:
USDOT_RSU-Req_327-v001	Virtual Ethernet Interfaces: The roadside unit SHALL support multiple, independent IPv4 and IPv6 networks.	IPv4, IPv6, and IEEE 802.3	Test:
USDOT_RSU-Req_584-v002	Interfaces: If the roadside unit contains additional integrated wireless interfaces, such as: -802.11b/g/n/a/acother Wi-Fi -Cellular 3G/4G -others those interfaces SHALL be inhibited or implement equivalent security access controls, authentication, integrity, and confidentiality to the services available over the wired Power-over-Ethernet (PoE) interface.		Test:
USDOT_RSU-Req_354-v001	Interfaces: The roadside unit SHOULD support NAT64 protocol		Test: If available

Dedicated Short-Range Communications

Table 3-23. DSRC Requirements.

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_367-v001	FCC Regulation 47 CFR Compliance: The roadside unit SHALL comply with Federal Communications Commission (FCC) Code of Federal Regulations Title 47 Parts 0, 1, 2, 15, 90, and 95.	Federal Communications Commission (FCC) Code of Federal Regulations Title 47 Parts 0, 1, 2, 15, 90, and 95	Test:

802.11

Table 3-24. IEEE 802.11 Requirements.

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_372-v002	IEEE 802.11 Conformance: The roadside unit SHALL conform to IEEE Std. 802.11 with Management Information Base (MIB) variable dot11OCBActivated set to "true" and as bounded by the general requirement to fully support the IEEE 1609.x protocol specification set.	802.11-2012 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, or later	Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_373-v003	IEEE 802.11 Physical Layer: The roadside unit SHALL implement the Orthogonal frequency division multiplexing (OFDM) physical layer of the Open Systems Interconnection (OSI) model defined in Clause 18 of IEEE 802.11, unless otherwise indicated (including all data rates for 10 MHz channel spacing and 20 MHz channel spacing in 18.2.3.4).	802.11-2012 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, or later, Clause 18	Test:
USDOT_RSU-Req_375-v001	IEEE 802.11 Default Values: The roadside unit SHALL use the default values defined in IEEE 802.11 unless otherwise indicated (including the slot time in 18.3.8.7).	802.11-2012 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, or later	Test:
USDOT_RSU-Req_376-v001	IEEE 802.11 Quality of Service: The roadside unit SHALL send 802.11 data frames using the Quality of Service (QoS) Data subtype.	802.11-2012 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, or later	Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_377-v001	Arbitration Interframe Spacing Value: The roadside unit SHALL configure an AIFSN of a given access category with an integer value from 2 to X, where the value of X is based on the chip set used – as defined by the vendor. Note: Vendor should provide the limit for X, based on the chip set used	802.11-2012 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, or later	Test:
USDOT_RSU-Req_378-v001	Transmission Opportunity Value: The TXOP Limit of a given AC SHALL be capable of being set to 0.	802.11-2012 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, or later	Test:
USDOT_RSU-Req_379-v001	Contention Window Minimum Value: The CWmin of a given AC SHALL take any value of the form (2^k)-1, for k = 1 through Y. Note: Vendor should provide the limit for Y, based on the chip set used.	802.11-2012 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, or later	Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_382-v001	IEEE 802.11 Basic Service Set: The roadside unit SHALL send MAC Protocol data units (MPDUs) outside the context of a basic service set (BSS), i.e. with Management Information Base (MIB) variable dot11OCBActivated is set to "true."	802.11-2012 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, or later	Test:
USDOT_RSU-Req_383-v001	IEEE 802.11 Operating Class 17: The roadside unit SHALL support Operating class 17 (even 10 MHz channels in the range 172 to 184).	802.11-2012 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, or later, Table E-1	Test:
USDOT_RSU-Req_384-v003	IEEE 802.11 Operating Class 18: The roadside unit SHALL support Operating class 18 (odd 20 MHz channels in the range 175 to 181).	802.11-2012 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, or later, Table E-1 FCC Title 47, Part 90.377	Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_385-v001	IEEE 802.11 Enhanced Distributed Channel Access: The roadside unit SHALL have a configurable EDCA parameter with a default as defined in IEEE 802.11.	802.11-2012 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, or later, Table 8-106	Test:

IEEE 1609.2

Table 3-25. IEEE 1609.2 Requirements.

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_388-v002	IEEE 1609.2 Conformance: The roadside unit SHALL conform to IEEE 1609.2	IEEE 1609.2-2016 IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages, as modified by guidance notes, or later	Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_578-v001	USDOT Security Credential Management System Conformance: The roadside unit SHALL conform to the USDOT Security Credential Management System End Entity Requirements.	USDOT Security Credential Management System Design: Security Credential Management System Proof–of–Concept Implementation EE Requirements and Specifications Supporting SCMS Software Release 1.1, published May, 2016, or later	Test:
USDOT_RSU-Req_579-v001	Secure Storage: The roadside unit SHOULD store all digital certificates and public and private key pars in secure storage, such as that contained in a Hardware Security Module.	USDOT Security Credential Management System Design: Security Credential Management System Proof–of–Concept Implementation EE Requirements and Specifications Supporting SCMS Software Release 1.1, published May, 2016, or later	Documentation:

IEEE 1609.3

Table 3-26. IEEE 1609.3 Requirements.

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_412-v002	IEEE 1609.3 Conformance: The roadside unit SHALL conform to IEEE 1609.3.	IEEE 1609.3-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services. or later	Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_413-v001	IEEE 1609.3 IP Data: The roadside unit SHALL process both transmitted and received IPv6 packets. Note: At a minimum, IP based communications over DSRC will be used for the exchange of data between the onboard equipment and the 1609.2 security credential management system.	IEEE 1609.3-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services. or later	Test:
USDOT_RSU-Req_414-v001	IEEE 1609.3 WSMP Data: The roadside unit SHALL process (both transmit and receive) WAVE Short Message Protocol (WSMP) messages.	IEEE 1609.3-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services. or later	Test:
USDOT_RSU-Req_415-v001	IEEE 1609.3 PSID-Specific User Priority: The roadside unit SHALL assign a configurable PSID value (default to the value specified for the associated application area defined in IEEE 1609.12-2016, or later) and a configurable User Priority value (default to 2) to each data frame.	IEEE 1609.3-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services. or later, IEEE P1609.12-2016 or later	Test:
USDOT_RSU-Req_416-v001	IEEE 1609.3 WSMP-N- Header Options: The following WSMP-N- header options SHALL be configured on the roadside unit: Data Rate Transmit Power Used	IEEE 1609.3-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services. or later	Test:

WAVE Service Advertisements

Appendix D contains an Example WSA for an RSU advertising Intersection.

Table 3-27. WSA Requirements.

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_586-v001	WSA Security Profile: The roadside unit SHALL conform to the WAVE Service Advertisement (WSA) Security Profile defined in IEEE 1609.3-2016 Annex H.1	IEEE 1609.3-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services	Test:
USDOT_RSU-Req_587-v001	WSA Broadcast Channel: The roadside unit SHALL broadcast WAVE Service Advertisements (WSA) on the Control Channel (CCH)	IEEE 1609.3-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services	Test:
USDOT_RSU-Req_588-v001	WSA Broadcast Time Slot: the roadside Unit SHALL broadcast WAVE Service Advertisements (WSA) during Time Slot 0	IEEE 1609.3-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services	Test:
USDOT_RSU-Req_570-v002	WSA Configuration_General: The roadside unit WAVE Service Advertisement (WSA) SHALL include DSRC Service Channel (SCH) Services from WSA MIB OID 1.0.15628.4.1.13		Test:
USDOT_RSU-Req_571-v001	WSA Configuration_S&R Messages: The roadside unit WAVE Service Advertisement (WSA) SHALL include DSRC Service Channel (SCH) Services based on the Store and Repeat messages contained in MIB OID 1.0.15628.4.1.4		Test:
USDOT_RSU-Req_572-v001	WSA Configuration_IF Messages: The roadside unit WAVE Service Advertisement (WSA) SHALL include DSRC Service Channel (SCH) Services based on Immediate Forward messages received on non-DSRC interfaces as listed in MIB OID 1.0.15628.4.1.5		Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_573-v002	Control Channel Store & Repeat Messages: Store & Repeat messages transmitted on the DSRC Control Channel (CCH), 178 SHALL NOT be included in the WAVE Service Advertisement		Test:
USDOT_RSU-Req_574-v001	Control Channel Immediate Forward Messages: Immediate Forward messages transmitted on the DSRC Control Channel (CCH), 178 SHALL NOT be included in the WAVE Service Advertisement		Test:

IEEE 1609.4

Table 3-28. IEEE 1609.4 Requirements.

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_419-v001	IEEE 1609.4 Standard Conformance: Each DSRC radio contained in the roadside unit SHALL conform to IEEE 1609.4.	IEEE 1609.4-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation, or later	Test:
USDOT_RSU-Req_420-v002	IEEE 1609.4 Radio Operating Modes: Each DSRC radio in the roadside unit SHALL be configurable to operate either in "Continuous" (operating continuously on a single Service Channel) or "Alternating" (switched between two Service Channels (or the Control Channel and a Service Channel)) Mode, as shown in Figure 9 of IEEE 1609.4-2016.	IEEE 1609.4-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation, Figure 9, or later	Test:
USDOT_RSU-Req_360-v002	Channel Modes: The roadside unit SHALL support Continuous Mode and Alternating Mode radio operations simultaneously	USDOT_RSU-Req_420-v001	Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_421-v001	IEEE 1609.4 Radio Channel Usage: Each DSRC radio in the roadside unit SHALL be configurable to send messages either on Channel 178 during the Control Channel (CCH) interval or on any of the 10 MHz or 20 MHz channels with no time interval restrictions.	IEEE 1609.4-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation, or later	Test:
USDOT_RSU-Req_422-v001	IEEE 1609.4 Continuous Channel Mode: Roadside unit DSRC Radios in Continuous Mode SHALL be configurable for operation on any 10 MHz or 20 MHz channel (default 10 MHz Channel 172) with no time interval restrictions.	IEEE 1609.4-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation, or later	Test:
USDOT_RSU-Req_423-v001	IEEE 1609.4 CCH Alternating Channel Mode: Roadside unit DSRC Radios in Alternating Mode SHALL broadcast WAVE Service Advertisements and WAVE Short Messages on Channel 178 during the Control Channel (CCH) interval	IEEE 1609.4-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation, or later	Test:
USDOT_RSU-Req_436-v001	IEEE 1609.4 SCH Alternating Channel Mode: Roadside unit DSRC Radios in Alternating Mode SHALL be configurable to operate on any 10 MHz or 20 MHz channel during the Service Channel (SCH) Interval. Note: Service Channel configuration is part of the SNMPv3 MIB, see Appendix B.	IEEE 1609.4-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation, or later	Test:
USDOT_RSU-Req_424-v002	Service Channel Interval: Roadside unit DSRC Radios in Alternating Mode SHALL be capable of switching to the configured Service Channel every Service Channel interval with no time interval restrictions.	IEEE 1609.4-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation, or later	Test:

ReqID	Description	Reference	Verification Method
USDOT_RSU-Req_425-v002	RSU Sets-Service Channel Alternating Mode: All non-master roadside unit DSRC radios in Alternating Mode within the same RSU set SHALL automatically operate on the same service channel(s) as the configuration of the “master” roadside unit.	IEEE 1609.4-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation, or later	Test:
USDOT_RSU-Req_429-v001	IEEE 1609.4 Synchronized Collision: Roadside unit DSRC radios in Alternating Mode SHALL avoid the synchronized collision phenomenon described in Annex B of IEEE 1609.4 when broadcasting messages on during the Control Channel interval.	IEEE 1609.4-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation, Annex B, or later	Test:
USDOT_RSU-Req_430-v001	IEEE 1609.4 Readdressing Option: The roadside unit SHALL implement the readdressing option defined in IEEE 1609.4	IEEE 1609.4-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation Clause 6.6, or later	Test:

Appendix A. Terms and Definitions

Term	Definition
AASHTO	American Association of State Highway and Transportation Officials
ACL	Access Control List
AIFSN	Arbitration Interframe Space Number, See IEEE 802.11
BSM	Basic Safety Message
C	Celsius (Unit of Temperature)
CA	Certificate Authority
CAMP	Crash Avoidance Metrics Partnership
CCH	Control Channel
CFR	Code of Federal Regulations
Channel Mode	Single Channel Continuous or Dual Channel Alternating as defined in IEEE 1609.4.
CML	Communications Message Log
CRL	Certificate Revocation List
CSW	Curve Speed Warning
CWmin	Contention Window Minimum Size
dBm	Decibel-milliwatts
DARPA	Defense Advanced Research Projects Agency
DC	Direct Current
DSRC	Dedicated Short-Range Communication
EDCA	Enhanced Distributed Channel Access
EMI	Electromagnetic Interference
FCC	Federal Communications Commission
GHz	Gigahertz
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
Immediate Forward Messages	Dynamic messages from ancillary devices connected to an RSU. An Example would be SPaT. The RSU transmits Immediate Forward messages only when the RSU receives them.

Term	Definition
IPv6	Internet Protocol version 6 (IPv6) is a protocol upgrade of for IPv4 (the current basis of the internet. IPv6 uses 128 bit addresses as opposed to the 32 bit IPv4 address. The basics of IPv6 are similar to those of IPv4 -- devices can use IPv6 as source and destination addresses to pass packets over a network, and tools like ping work for network testing as they do in IPv4, with some slight variations, however network appliance (switches, routers, firewalls, etc.) must specifically support IPv6.
IETF	Internet Engineering Task Force
ITS	Intelligent Transportation Systems
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Media Access Control
MB	Megabyte
MIB	Management Information Base
MHz	Megahertz
MPDUs	MAC Protocol Units
MTBF	Mean Time Between Failure
NEMA	National Electrical Manufacturers Association
NTCIP	National Transportation Communications for Intelligent Transportation System Protocol
NTP	Network Time Protocol
OID	Object Identifier (SNMP MIB OID)
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
PHY	Physical Layer, refers to a specific layer in the Open Systems Interconnection (OSI) reference model
PoE	Power-over-Ethernet
PSID	Provider Service Identifier
QoS	Quality of Service
RF	Radio Frequency
RFID	Radio Frequency Identification
Roadside Equipment	Traffic Management equipment installed along the roadside to convey traffic or traveler information to passing drivers or to connected said management equipment to a Traffic Management Center or other back office services and applications.
RSU	Roadside Unit
SAE	Society of Automotive Engineers
SCH	Service Channel

Term	Definition
SCMS	A Connected Vehicle Security Credential Management System (SCMS) provides DSRC devices with digital certificates that the devices use to sign (authenticate) and encrypt DSRC messages. The SCMS also revokes certificates, when warranted and provides a certificate revocation list (CRL) to remaining devices
SNMP	Simple Network Management Protocol
SPaT	Signal Phase and Timing
SSH	Secure Shell
Store and Repeat Messages	Static messages that are loaded on RSUs for transmission to passing vehicles. An Example would be a Curve Speed Warning (CSW) Message that contains the geometry of the subject curve and an advised speed in which to traverse the curve. These messages are loaded as individual text files that contain the transmission strategy (how often the message is transmitted, what (DSRC) channel the messages is transmitted on, etc.) and the message payload.
TLS	Transport Layer Security
TMC	Traffic Management Center
TXOP	Transmission Opportunity Value
USDOT	United States Department of Transportation
UTC	Universal Time, Coordinated
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
VSC3	Vehicle Safety Communications 3 (Consortium)
WAAS	Wide Area Augmentation System
WAVE	Wireless Access in Vehicular Environments
WiMAX	Worldwide Interoperability for Microwave Access
WSA	WAVE Service Announcement
WSM	WAVE Short Message
WSMP	WAVE Short Message Protocol

Appendix B. SNMPv3 Management Information Base

B.1. RSU Specific MIB Objects

This section contains the RSU specific MIB OIDs

```
RSU-MIB DEFINITIONS ::= BEGIN

IMPORTS
      MODULE-IDENTITY, OBJECT-TYPE, Integer32,
      Counter32, NOTIFICATION-TYPE        FROM SNMPv2-SMI
      TEXTUAL-CONVENTION, DateAndTime, RowStatus,
      PhysAddress, DisplayString, MacAddress          FROM SNMPv2-TC
      MODULE-COMPLIANCE, OBJECT-GROUP                 FROM SNMPv2-CONF
      Ipv6Address                                     FROM IPV6-TC;

rsuMIB MODULE-IDENTITY
      LAST-UPDATED      "201702200000Z"
      ORGANIZATION      "US-DOT"
      CONTACT-INFO      "postal:    TBD
                               email:           TBD@TBD.com"
      DESCRIPTION       "Leidos implementation RSU 4.1 MIB based on
                               Savari and Cohda implementation of RSU 4.0"
      REVISION          "201702200000Z"
      DESCRIPTION       "Corrections to INTEGER/Integer32 types and typos"
      REVISION          "201610310000Z"
      DESCRIPTION       "Final Draft for RSU 4.1 Spec."
      REVISION          "201608310230Z"
      DESCRIPTION       "Second Draft for RSU 4.1 Spec."
      REVISION          "201608120230Z"
      DESCRIPTION       "First Draft for RSU 4.1 Spec."
      REVISION          "201606270245Z"
      DESCRIPTION       "Combining input from Vendors"
      REVISION          "201404150000Z"            -- 15 April 2014 midnight
      DESCRIPTION       "RSU MIB Definitions"
      ::= { iso std(0) rsu(15628) version(4) 1 }



RsuTableIndex ::= TEXTUAL-CONVENTION
      DISPLAY-HINT   "d"
      STATUS         current
      DESCRIPTION
            "A valid range of values for use in table indices"
      SYNTAX         Integer32 (1..2147483647)

RsuPsidTC ::= TEXTUAL-CONVENTION
      DISPLAY-HINT   "2x"
      STATUS         current
      DESCRIPTION
            "PSID associated with a DSRC message."
```

```
      SYNTAX         OCTET STRING (SIZE(1..2))


rsuContMacAddress OBJECT-TYPE
    SYNTAX      MacAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
    "Represents an 802 MAC address of the DSRC Radio operating in
         Continuous Mode represented in the 'canonical' order defined by
         IEEE 802.1a, i.e., as if it were transmitted least significant
         bit first, even though 802.5 (in contrast to other 802.x protocols)
         requires MAC addresses to be transmitted most significant bit first"
    ::= { rsuMIB 1 }

-- add entries for multiple antennas

rsuAltMacAddress OBJECT-TYPE
    SYNTAX      MacAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Represents an 802 MAC address of the DSRC Radio operating in
         Alternating Mode represented in the 'canonical' order defined
         by IEEE 802.1a, i.e., as if it were transmitted least significant
         bit first, even though 802.5 (in contrast to other 802.x protocols)
         requires MAC addresses to be transmitted most significant bit first"
    ::= { rsuMIB 2 }


rsuGpsStatus OBJECT-TYPE
      SYNTAX       Integer32 (0..15)
      MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
      "Provides the number of GPS Satellites RSUxs internal GPS receiver is
            tracking"
      ::= { rsuMIB 3 }


rsuSRMStatusTable OBJECT-TYPE
      SYNTAX SEQUENCE OF RsuSRMStatusEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Provides configuration information for each Store
            Repeat message sent by an RSU."
      ::= { rsuMIB 4 }


rsuSRMStatusEntry OBJECT-TYPE
      SYNTAX RsuSRMStatusEntry
      MAX-ACCESS  not-accessible
      STATUS      current
```

```
      DESCRIPTION
                  "A row describing RSU Store and Repeat Message Status"
      INDEX   { rsuSRMIndex }
      ::= {rsuSRMStatusTable 1 }


RsuSRMStatusEntry ::= SEQUENCE {
        rsuSRMIndex             RsuTableIndex,
        rsuSRMPsid              RsuPsidTC,
        rsuSRMDsrcMsgId         Integer32,
        rsuSRMTxMode            INTEGER,
        rsuSRMTxChannel         Integer32,
        rsuSRMTxInterval        Integer32,
        rsuSRMDeliveryStart     OCTET STRING,
        rsuSRMDeliveryStop      OCTET STRING,
        rsuSRMPayload           OCTET STRING,
        rsuSRMEnable            INTEGER,
        rsuSRMStatus            RowStatus
    }

rsuSRMIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "Store and Repeat Message Index "
    ::= { rsuSRMStatusEntry 1 }

rsuSRMPsid OBJECT-TYPE
    SYNTAX       RsuPsidTC
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Store and Repeat Message PSID"
    ::= { rsuSRMStatusEntry 2 }

rsuSRMDsrcMsgId OBJECT-TYPE
    SYNTAX       Integer32
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Store and Repeat Message DSRC Message ID"
    ::= { rsuSRMStatusEntry 3 }

rsuSRMTxMode OBJECT-TYPE
      SYNTAX       INTEGER { cont(0), alt(1) }
      MAX-ACCESS   read-create
      STATUS       current
      DESCRIPTION
            "DSRC mode set for Store and Repeat Message transmit,
             Continuous or Alternating"
      ::= { rsuSRMStatusEntry 4 }

rsuSRMTxChannel OBJECT-TYPE
```

```
    SYNTAX       Integer32 (172..184)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "DSRC channel set for Store and Repeat Message transmit"
    ::= { rsuSRMStatusEntry 5 }

rsuSRMTxInterval OBJECT-TYPE
    SYNTAX       Integer32 (1..2147483647)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Time interval in milliseconds between two successive
             Store and Repeat Messages"
    ::= { rsuSRMStatusEntry 6 }

rsuSRMDeliveryStart OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(0|6))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Store and Repeat Message delivery start time"
    ::= { rsuSRMStatusEntry 7 }

rsuSRMDeliveryStop OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(0|6))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Store and Repeat Message delivery stop time"
      ::= { rsuSRMStatusEntry 8 }

rsuSRMPayload OBJECT-TYPE
      SYNTAX       OCTET STRING (SIZE(0..1500))
      MAX-ACCESS   read-create
      STATUS       current
      DESCRIPTION
            "Payload of Store and Repeat message.
            Length limit derived from UDP size limit."
      ::= { rsuSRMStatusEntry 9 }

rsuSRMEnable OBJECT-TYPE
      SYNTAX       INTEGER { off(0), on(1) }
      MAX-ACCESS   read-create
      STATUS       current
      DESCRIPTION
            "Set this bit to enable transmission of the message
             0=off, 1=on"
      ::= { rsuSRMStatusEntry 10 }

rsuSRMStatus OBJECT-TYPE
      SYNTAX       RowStatus
      MAX-ACCESS   read-create
      STATUS       current
```

```
      DESCRIPTION
            "create and destroy row entry"
      ::= { rsuSRMStatusEntry 11 }


rsuIFMStatusTable OBJECT-TYPE
    SYNTAX SEQUENCE OF RsuIFMStatusEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Provides configuration parameters for each Immediate
        Forward message sent by an RSU."
    ::= { rsuMIB 5 }

rsuIFMStatusEntry OBJECT-TYPE
    SYNTAX       RsuIFMStatusEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "A row describing RSU Immediate Forward Message Status"
    INDEX   { rsuIFMIndex }
    ::= {rsuIFMStatusTable 1 }

RsuIFMStatusEntry ::= SEQUENCE {
    rsuIFMIndex             RsuTableIndex,
    rsuIFMPsid              RsuPsidTC,
    rsuIFMDsrcMsgId         Integer32,
      rsuIFMTxMode            INTEGER,
    rsuIFMTxChannel         Integer32,
      rsuIFMEnable            INTEGER,
      rsuIFMStatus            RowStatus
    }


rsuIFMIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "Immediate Forward Message Index "
    ::= { rsuIFMStatusEntry 1 }


rsuIFMPsid OBJECT-TYPE
    SYNTAX       RsuPsidTC
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Immediate Forward Message PSID"
    ::= { rsuIFMStatusEntry 2}


rsuIFMDsrcMsgId OBJECT-TYPE
    SYNTAX       Integer32
```

```
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Immediate Forward Message DSRC Message ID"
    ::= { rsuIFMStatusEntry 3 }

rsuIFMTxMode OBJECT-TYPE
      SYNTAX       INTEGER { cont(0), alt(1) }
      MAX-ACCESS   read-create
      STATUS       current
      DESCRIPTION
            "Immediate Forward Message Transmit Mode
             Alternating or Continuous"
      ::= { rsuIFMStatusEntry 4 }

rsuIFMTxChannel OBJECT-TYPE
    SYNTAX       Integer32 (172..184)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "DSRC channel set for Immediate Forward Message transmit"
    ::= { rsuIFMStatusEntry 5 }

rsuIFMEnable OBJECT-TYPE
    SYNTAX       INTEGER { off(0), on(1) }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Set this bit to enable transmission of the message
             0=off, 1=on"
    ::= { rsuIFMStatusEntry 6 }

rsuIFMStatus OBJECT-TYPE
      SYNTAX       RowStatus
      MAX-ACCESS   read-create
      STATUS       current
      DESCRIPTION
            "create and destroy row entry"
      ::= { rsuIFMStatusEntry 7}


rsuSysObjectID OBJECT-TYPE
    SYNTAX       OBJECT IDENTIFIER
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
       "The vendor's authoritative identification of the network
        management subsystem contained in the entity. This value
        is allocated within the DSRC subtree (1.0.15628.4) and
        provides an easy and unambiguous means for determining
        `what kind of box' is being managed. 1.0.15628.4.1.6.0
        indicates an RSU"
    ::= { rsuMIB 6 }
```

```
rsuDsrcForwardTable OBJECT-TYPE
    SYNTAX SEQUENCE OF RsuDsrcForwardEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "contains the DSRC PSID being forwarded to a network host,
        the IP Address and port number of the destination host, as
        well as other configuration parameters as defined."
    ::= { rsuMIB 7}


rsuDsrcForwardEntry OBJECT-TYPE
    SYNTAX       RsuDsrcForwardEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "A row describing RSU Message Forwarding"
    INDEX   { rsuDsrcFwdIndex }
    ::= {rsuDsrcForwardTable 1 }


RsuDsrcForwardEntry ::= SEQUENCE {
      rsuDsrcFwdIndex              RsuTableIndex,
      rsuDsrcFwdPsid               RsuPsidTC,
      rsuDsrcFwdDestIpAddr         Ipv6Address,
      rsuDsrcFwdDestPort           Integer32,
      rsuDsrcFwdProtocol           INTEGER,
      rsuDsrcFwdRssi               Integer32,
      rsuDsrcFwdMsgInterval        Integer32,
      rsuDsrcFwdDeliveryStart      OCTET STRING,
      rsuDsrcFwdDeliveryStop       OCTET STRING,
      rsuDsrcFwdEnable             INTEGER,
      rsuDsrcFwdStatus             RowStatus
}

rsuDsrcFwdIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "Message Forward Message Index "
    ::= { rsuDsrcForwardEntry 1 }

rsuDsrcFwdPsid OBJECT-TYPE
    SYNTAX       RsuPsidTC
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "DSRC Message Forward PSID"
    ::= { rsuDsrcForwardEntry 2 }


rsuDsrcFwdDestIpAddr OBJECT-TYPE
```

```
    SYNTAX       Ipv6Address
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "DSRC Message Forward Destination Server IP address"
    ::= { rsuDsrcForwardEntry 3 }


rsuDsrcFwdDestPort OBJECT-TYPE
    SYNTAX       Integer32 (1024 .. 65535)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "DSRC Message Forward Destination Server Port Number"
    ::= { rsuDsrcForwardEntry 4 }

rsuDsrcFwdProtocol OBJECT-TYPE
    SYNTAX       INTEGER { tcp(1), udp(2) }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "DSRC Message Forward Transport Protocol between RSU and Server"
    ::= { rsuDsrcForwardEntry 5 }

rsuDsrcFwdRssi OBJECT-TYPE
    SYNTAX       Integer32 (-100 .. -60)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Minimum Received Signal Strengh Level of DSRC Messages should be
        Forwarded to server"
    ::= { rsuDsrcForwardEntry 6 }

rsuDsrcFwdMsgInterval OBJECT-TYPE
    SYNTAX       Integer32 (1 .. 9)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Interval with which RSU forwards DSRC Messages to Server"
    ::= { rsuDsrcForwardEntry 7 }

rsuDsrcFwdDeliveryStart OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(0|6))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Start time for RSU to start forwarding DSRC Messages to Server"
    ::= { rsuDsrcForwardEntry 8 }


rsuDsrcFwdDeliveryStop OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(0|6))
    MAX-ACCESS   read-create
    STATUS       current
```

```
    DESCRIPTION
        "Stop time for RSU to stop forwarding DSRC Messages to Server"
    ::= { rsuDsrcForwardEntry 9 }

rsuDsrcFwdEnable OBJECT-TYPE
    SYNTAX       INTEGER { off(0), on(1) }
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Stop time for RSU to stop forwarding DSRC Messages to Server"
    ::= { rsuDsrcForwardEntry 10 }

rsuDsrcFwdStatus OBJECT-TYPE
    SYNTAX       RowStatus
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "create and destroy row entry "
    ::= { rsuDsrcForwardEntry 11 }


rsuGpsOutput OBJECT IDENTIFIER ::= { rsuMIB 8 }

rsuGpsOutputPort OBJECT-TYPE
    SYNTAX       Integer32 (1024 .. 65535)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "GPS Out External Server Port Number"
      ::= { rsuGpsOutput 1 }

rsuGpsOutputAddress OBJECT-TYPE
      SYNTAX       Ipv6Address
      MAX-ACCESS   read-write
      STATUS       current
      DESCRIPTION
            "Remote host IPv6 address to which to send the GPS string"
      ::= { rsuGpsOutput 2 }

rsuGpsOutputInterface OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   read-write
      STATUS       current
      DESCRIPTION
            "Local interface on which to output the GPS string"
      ::= { rsuGpsOutput 3 }

rsuGpsOutputInterval OBJECT-TYPE
      SYNTAX       Integer32 (1..18000)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Interval at which to send the GPS GPGGA NMEA String
        to external Server in seconds."
```

```
      ::= { rsuGpsOutput 4 }

rsuGpsOutputString OBJECT-TYPE
      SYNTAX       DisplayString (SIZE(0..100))
      MAX-ACCESS   read-only
      STATUS       current
      DESCRIPTION
            "Contains GPS NMEA GPGGA output string"
      ::= { rsuGpsOutput 5 }

rsuGpsRefLat OBJECT-TYPE
      SYNTAX       Integer32 (-900000000..900000000)
      MAX-ACCESS   read-write
      STATUS       current
      DESCRIPTION
            "Contains the actual GPS latitude for validation of
             reported GPS latitude in 10^-7 degrees."
      ::= { rsuGpsOutput 6 }

rsuGpsRefLon OBJECT-TYPE
      SYNTAX       Integer32 (-1800000000..1800000000)
      MAX-ACCESS   read-write
      STATUS       current
      DESCRIPTION
            "Contains the actual GPS longitude for validation of
             reported GPS longitude in 10^-7 degrees."
      ::= { rsuGpsOutput 7 }

rsuGpsRefElv OBJECT-TYPE
      SYNTAX       Integer32 (-100000..1000000)
      MAX-ACCESS   read-write
      STATUS       current
      DESCRIPTION
            "Contains the actual GPS elevation for validation of
             reported GPS elevation in centimeters."
      ::= { rsuGpsOutput 8 }

rsuGpsMaxDeviation OBJECT-TYPE
      SYNTAX       Integer32 (1..2000000)
      MAX-ACCESS   read-write
      STATUS       current
      DESCRIPTION
            "Contains the maximum allowable deviation (radius in centimeters)
             for comparison between the reported GPS coordinates and the
             static GPS coordinates."
      ::= { rsuGpsOutput 9 }


rsuInterfaceLogTable OBJECT-TYPE
    SYNTAX       SEQUENCE OF RsuInterfaceLogEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "Provides configuration information for capturing log files
```

```
        for each communication Interface x represents the
        interface for which these configurations will apply"
    ::= { rsuMIB 9 }

rsuInterfaceLogEntry OBJECT-TYPE
    SYNTAX       RsuInterfaceLogEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "A row describing RSU Interface Log"
    INDEX   { rsuIfaceLogIndex }
    ::= {rsuInterfaceLogTable 1 }

RsuInterfaceLogEntry ::= SEQUENCE {
        rsuIfaceLogIndex             RsuTableIndex,
        rsuIfaceGenerate             INTEGER,
        rsuIfaceMaxFileSize          Integer32,
        rsuIfaceMaxFileTime          Integer32,
            rsuIfaceLogByDir             INTEGER,
            rsuIfaceName                 DisplayString
   }

rsuIfaceLogIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        " Interface Logging Index "
    ::= { rsuInterfaceLogEntry 1 }

rsuIfaceGenerate OBJECT-TYPE
    SYNTAX INTEGER { off(0),
                     on(1) }
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Enable / Disable interface logging. '0x00 = OFF' and
        '0x01 = ON'"
    ::= { rsuInterfaceLogEntry 2 }

rsuIfaceMaxFileSize OBJECT-TYPE
    SYNTAX Integer32 (1..40)
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Maximum Interface Log File Size in Mega Bytes,
             default is 5."
    ::= { rsuInterfaceLogEntry 3 }

rsuIfaceMaxFileTime OBJECT-TYPE
    SYNTAX Integer32 (1..48)
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
```

```
        "Maximum Collection time for Interface Logging in hrs,
             default is 24."
    ::= { rsuInterfaceLogEntry 4 }

rsuIfaceLogByDir OBJECT-TYPE
    SYNTAX       INTEGER { off(0), on(1) }
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Sets whether or not to separate the log files by direction."
    ::= { rsuInterfaceLogEntry 5 }

rsuIfaceName OBJECT-TYPE
    SYNTAX       DisplayString
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Holds the name of the interface."
    ::= { rsuInterfaceLogEntry 6 }


rsuSecCredReq OBJECT-TYPE
    SYNTAX OCTET STRING (SIZE (1))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
      "rovides configuration parameters for when an RSU should
        request new 1609.2 security credentials in days before
        existing credentials expire"
    ::= { rsuMIB 10 }


rsuSecCredAttachInterval OBJECT-TYPE
    SYNTAX     Integer32 (1..100)
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Provides configuration parameters for when an RSU will attach
        1609.2 security credentials to a WAVE Short Message Protocol
        (WSMP) Message"
    ::= { rsuMIB 11 }


rsuDsrcChannelModeTable OBJECT-TYPE
    SYNTAX SEQUENCE OF RsuDsrcChannelModeEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
      "Provides Continuous and Alternating Channel Mode
        configurations for each DSRC interface.
        x represents the interface for which these
        configurations will apply"
    ::= { rsuMIB 12  }
```

```
rsuDsrcChannelModeEntry OBJECT-TYPE
    SYNTAX RsuDsrcChannelModeEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A row describing RSU Interface Log"
    INDEX   { rsuDCMIndex }
    ::= {rsuDsrcChannelModeTable 1 }

RsuDsrcChannelModeEntry ::= SEQUENCE {
      rsuDCMIndex       RsuTableIndex,
      rsuDCMRadio       DisplayString,
      rsuDCMMode        INTEGER,
    rsuDCMCCH         Integer32,
    rsuDCMSCH         Integer32
    }

rsuDCMIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        " Radio Interface Channel Mode Index "
    ::= { rsuDsrcChannelModeEntry 1 }

rsuDCMRadio OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   read-only
      STATUS       current
      DESCRIPTION
            "Name of the radio that the configuration relates to."
      ::= { rsuDsrcChannelModeEntry 2 }

rsuDCMMode OBJECT-TYPE
    SYNTAX       INTEGER { cont(0), alt(1) }
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
            "DSRC Channel Mode. '0x00 = Continuous Mode'
         and, '0x01 = Alternating Mode'"
    ::= { rsuDsrcChannelModeEntry 3 }

rsuDCMCCH OBJECT-TYPE
    SYNTAX       Integer32 (172..184)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Control Channel number to use - applies in Alternating Mode"
    ::= { rsuDsrcChannelModeEntry 4 }

rsuDCMSCH OBJECT-TYPE
    SYNTAX       Integer32 (172..184)
    MAX-ACCESS   read-write
    STATUS       current
```

```
    DESCRIPTION
        "Service Channel number to use"
    ::= { rsuDsrcChannelModeEntry 5 }


rsuWsaServiceTable OBJECT-TYPE
    SYNTAX SEQUENCE OF RsuWsaServiceEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Holds general configuration parameters for the RSU WAVE
         Service Advertisement."
    ::= { rsuMIB 13 }

rsuWsaServiceEntry OBJECT-TYPE
    SYNTAX RsuWsaServiceEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A row describing RSU WSA Service "
    INDEX   { rsuWsaIndex }
    ::= {rsuWsaServiceTable 1 }

RsuWsaServiceEntry ::= SEQUENCE {
        rsuWsaIndex                 RsuTableIndex,
        rsuWsaPsid                  RsuPsidTC,
        rsuWsaPriority              Integer32,
        rsuWsaProviderContext       OCTET STRING,
        rsuWsaIpAddress             Ipv6Address,
        rsuWsaPort                  Integer32,
            rsuWsaChannel               Integer32,
          rsuWsaStatus                RowStatus
    }

rsuWsaIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        " WSA Service Index "
    ::= { rsuWsaServiceEntry 1 }

rsuWsaPsid OBJECT-TYPE
      SYNTAX       RsuPsidTC
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "WSA Service PSID"
    ::= { rsuWsaServiceEntry 2 }

rsuWsaPriority OBJECT-TYPE
    SYNTAX       Integer32 (0 .. 63)
    MAX-ACCESS   read-create
    STATUS       current
```

```
    DESCRIPTION
        "Priority of WSA Service Advertised "
    ::= { rsuWsaServiceEntry 3 }

rsuWsaProviderContext OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE (4))
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "WSA Service Specific Provider Context "
    ::= { rsuWsaServiceEntry 4 }

rsuWsaIpAddress OBJECT-TYPE
    SYNTAX       Ipv6Address
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "IPv6 address of WSA Service Advertised "
    ::= { rsuWsaServiceEntry 5 }

rsuWsaPort OBJECT-TYPE
    SYNTAX       Integer32 (1024 .. 65535)
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Port Number of WSA Service Advertised "
    ::= { rsuWsaServiceEntry 6 }

rsuWsaChannel OBJECT-TYPE
      SYNTAX       Integer32 (172..184)
      MAX-ACCESS   read-create
      STATUS       current
      DESCRIPTION
            "The number of the channel on which the advertised service is
provided."
      ::= { rsuWsaServiceEntry 7 }

rsuWsaStatus OBJECT-TYPE
      SYNTAX       RowStatus
      MAX-ACCESS   read-create
      STATUS       current
      DESCRIPTION
            "create or destroy rows"
      ::= { rsuWsaServiceEntry 8 }


rsuWraConfiguration OBJECT IDENTIFIER ::= { rsuMIB 14 }

rsuWraIpPrefix OBJECT-TYPE
    SYNTAX       Ipv6Address
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "IPv6 address prefix of WRA Service Advertised "
```

```
    ::= { rsuWraConfiguration 1 }

rsuWraIpPrefixLength OBJECT-TYPE
    SYNTAX       OCTET STRING (SIZE(1))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Length of IPv6 address prefix of WRA Service Advertised "
    ::= { rsuWraConfiguration 2 }

rsuWraGateway OBJECT-TYPE
      SYNTAX       Ipv6Address
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "IPv6 address of Gateway of WRA Service Advertised "
    ::= { rsuWraConfiguration 3 }

rsuWraPrimaryDns OBJECT-TYPE
      SYNTAX       Ipv6Address
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "IPv6 address of Primary DNS Server of WRA Service Advertised "
    ::= { rsuWraConfiguration 4 }


rsuMessageStats OBJECT IDENTIFIER ::= { rsuMIB 15 }

rsuAltSchMsgSent OBJECT-TYPE
    SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages sent on Alternating Service Channel since
             start of service."
    ::= { rsuMessageStats 1 }

rsuAltSchMsgRcvd OBJECT-TYPE
      SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages received on Alternating Service Channel since
             start of service."
    ::= { rsuMessageStats 2 }

rsuAltCchMsgSent OBJECT-TYPE
      SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages sent on Alternating Control Channel since
             start of service."
```

```
    ::= { rsuMessageStats 3 }

rsuAltCchMsgRcvd OBJECT-TYPE
      SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages received on Alternating Control Channel since
             start of service."
    ::= { rsuMessageStats 4 }

rsuContSchMsgSent OBJECT-TYPE
      SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages sent on Continuous Service Channel since
             start of service."
    ::= { rsuMessageStats 5 }

rsuContSchMsgRcvd OBJECT-TYPE
      SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages received on Continuous Service Channel since
             start of service."
    ::= { rsuMessageStats 6 }

rsuContCchMsgSent OBJECT-TYPE
      SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages sent on Continuous Control Channel since
             start of service."
    ::= { rsuMessageStats 7 }

rsuContCchMsgRcvd OBJECT-TYPE
      SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Number of messages sent on Continuous Control Channel since
             start of service."
    ::= { rsuMessageStats 8 }

rsuMessageCountsByPsidTable OBJECT-TYPE
    SYNTAX SEQUENCE OF RsuMessageCountsByPsidEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Provides a count of transmitted messages sorted by PSID.
             Each row is a different PSID."
```

```
    ::= { rsuMessageStats 9 }

rsuMessageCountsByPsidEntry OBJECT-TYPE
    SYNTAX RsuMessageCountsByPsidEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A row describing the number of messages transmitted "
    INDEX   { rsuMessageCountsByPsidIndex }
    ::= { rsuMessageCountsByPsidTable 1 }

RsuMessageCountsByPsidEntry ::= SEQUENCE {
      rsuMessageCountsByPsidIndex        RsuTableIndex,
      rsuMessageCountsByPsidId           RsuPsidTC,
      rsuMessageCountsByPsidCounts       Counter32,
      rsuMessageCountsByPsidRowStatus    RowStatus
      }

rsuMessageCountsByPsidIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        " WSA Service Index "
    ::= { rsuMessageCountsByPsidEntry 1 }

rsuMessageCountsByPsidId OBJECT-TYPE
      SYNTAX       RsuPsidTC
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the number of seconds that have elapsed
             since the RSU was last powered on."
    ::= { rsuMessageCountsByPsidEntry 2 }

rsuMessageCountsByPsidCounts OBJECT-TYPE
      SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the number of seconds that have elapsed
             since the RSU was last powered on."
    ::= { rsuMessageCountsByPsidEntry 3 }

rsuMessageCountsByPsidRowStatus OBJECT-TYPE
      SYNTAX       RowStatus
      MAX-ACCESS   read-create
      STATUS       current
      DESCRIPTION
            "create or destroy rows"
      ::= { rsuMessageCountsByPsidEntry 4 }


rsuSystemStats OBJECT IDENTIFIER ::= { rsuMIB 16 }
```

```
rsuTimeSincePowerOn OBJECT-TYPE
      SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the number of seconds that have elapsed
             since the RSU was last powered on."
    ::= { rsuSystemStats 1 }

rsuTotalRunTime OBJECT-TYPE
      SYNTAX       Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the number of seconds that have elapsed
             since the RSU was first powered on."
    ::= { rsuSystemStats 2 }

rsuLastLoginTime OBJECT-TYPE
      SYNTAX       DateAndTime
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the time when the last user logged in."
    ::= { rsuSystemStats 3 }

rsuLastLoginUser OBJECT-TYPE
      SYNTAX       DisplayString (SIZE(0..32))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the name of the last user to log in."
    ::= { rsuSystemStats 4 }

rsuLastLoginSource OBJECT-TYPE
      SYNTAX       DisplayString (SIZE(0..32))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains name or address of the remote host from which
             the last user logged in."
    ::= { rsuSystemStats 5 }

rsuLastRestartTime OBJECT-TYPE
      SYNTAX       DateAndTime
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the time when the RSU process was last started."
    ::= { rsuSystemStats 6 }

rsuIntTemp OBJECT-TYPE
      SYNTAX       Integer32 (-100..100)
```

```
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the internal temperature of the RSU in degrees Celsius."
    ::= { rsuSystemStats 7 }

rsuSysDescription OBJECT IDENTIFIER ::= { rsuMIB 17 }

rsuMibVersion OBJECT-TYPE
      SYNTAX       DisplayString (SIZE(0..32))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the version of this MIB."
    ::= { rsuSysDescription 1 }

rsuFirmwareVersion OBJECT-TYPE
      SYNTAX       DisplayString (SIZE(0..32))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the version of firmware running on this RSU."
    ::= { rsuSysDescription 2 }

rsuLocationDesc OBJECT-TYPE
      SYNTAX       DisplayString (SIZE(0..140))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains a description of the installation location of this RSU."
    ::= { rsuSysDescription 3 }

rsuID OBJECT-TYPE
      SYNTAX       DisplayString (SIZE(0..32))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the ID given to this RSU."
    ::= { rsuSysDescription 4 }

rsuManufacturer OBJECT-TYPE
      SYNTAX       DisplayString (SIZE(0..32))
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Contains the name of the manufacturer of this RSU."
    ::= { rsuSysDescription 5 }

rsuSysSettings OBJECT IDENTIFIER ::= { rsuMIB 18 }

rsuTxPower OBJECT-TYPE
      SYNTAX       Integer32 (0..100)
    MAX-ACCESS   read-write
    STATUS       current
```

```
    DESCRIPTION
        "Sets the output power of the RSU antennas as a
         percentage of full strength. Default is 100% of 33dBm."
    ::= { rsuSysSettings 1 }

rsuNotifyIpAddress OBJECT-TYPE
      SYNTAX       Ipv6Address
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the IP address of the SNMP Manager that will
         receive the SNMP Notifications."
    ::= { rsuSysSettings 2 }

rsuNotifyPort OBJECT-TYPE
      SYNTAX       Integer32 (0..65535)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the port number of the SNMP Manager that will
             receive the SNMP Notifications. Default is 162."
    ::= { rsuSysSettings 3 }

rsuSysLogCloseDay OBJECT-TYPE
      SYNTAX       INTEGER {  monday(1), tuesday(2), wednesday(3),
                              thursday(4), friday(5), saturday(6),
                              sunday(7) }
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the day of the week on which to close the system
             log file Default is Sunday."
    ::= { rsuSysSettings 4 }

rsuSysLogCloseTime OBJECT-TYPE
      SYNTAX       OCTET STRING (SIZE(3))
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the time of day at which to close the system
             log file. Default is 23:59:00 UTC."
    ::= { rsuSysSettings 5 }

rsuSysLogDeleteDay OBJECT-TYPE
      SYNTAX       INTEGER {  monday(1), tuesday(2), wednesday(3),
                              thursday(4), friday(5), saturday(6),
                              sunday(7) }
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the day of the week on which to close the system
             log file Default is Sunday."
    ::= { rsuSysSettings 6 }
```

```
rsuSysLogDeleteAge OBJECT-TYPE
      SYNTAX       Integer32
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the age at which to delete old log files.
             Default is 30 days."
    ::= { rsuSysSettings 7 }



-- System Status

rsuSystemStatus OBJECT IDENTIFIER ::= { rsuMIB 19}

rsuChanStatus OBJECT-TYPE
      SYNTAX INTEGER {
        bothOp (0), --both Continuous and Alternating modes are operational
        altOp (1),  --Alternating mode is operational,
                                --Continuous mode is not operational
        contOp (2), --Continuous mode is operational,
                                --Alternating mode is not operational
        noneOp (3)  --neither Continuous nor Alternating mode is operational
    }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Indicates which channel modes are operating.
             Note: Operating means the device is functioning
             as designed, configured, and intended"
    ::= { rsuSystemStatus 1 }



-- Situation Data

rsuSitData OBJECT IDENTIFIER ::= { rsuMIB 20 }

rsuSdcDestIpAddress OBJECT-TYPE
      SYNTAX       Ipv6Address
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the IPv6 address of the Situation Data Clearinghouse."
    ::= { rsuSitData 1 }

rsuSdcDestPort OBJECT-TYPE
      SYNTAX       Integer32 (1024..65535)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the port on which the Situation Data Clearinghouse
             will receive data."
    ::= { rsuSitData 2 }
```

```
rsuSdcInterval OBJECT-TYPE
      SYNTAX       Integer32 (1..18000)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the interval in seconds at which the RSU will send
             data to the Situation Data Clearinghouse."
    ::= { rsuSitData 3 }

rsuSdwIpAddress OBJECT-TYPE
      SYNTAX       Ipv6Address
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the IPv6 address of the Situation Data Warehouse."
    ::= { rsuSitData 4 }

rsuSdwPort OBJECT-TYPE
      SYNTAX       Integer32 (1024..65535)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "Contains the port on which the Situation Data Warehouse
             will receive requrests from the RSU."
    ::= { rsuSitData 5 }


-- RSU Set

rsuSet OBJECT IDENTIFIER ::= { rsuMIB 21 }

rsuSetRole OBJECT-TYPE
      SYNTAX       INTEGER {
                                    master (0),
                                    slave (1)
                           }
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "The role of the RSU in a set (master or slave)"
    ::= { rsuSet 1 }

rsuSetEnable OBJECT-TYPE
      SYNTAX       INTEGER {
                                    independent (0),
                                    set (1)
                           }
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
        "The status of the RSU set. 0 is not operating in a set;
             1 is operating in a set."
    ::= { rsuSet 2 }
```

```
rsuSetSlaveTable OBJECT-TYPE
    SYNTAX SEQUENCE OF RsuSetSlaveEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Holds the configuration parameters for the slave RSUs."
    ::= { rsuSet 3 }

rsuSetSlaveEntry OBJECT-TYPE
    SYNTAX      RsuSetSlaveEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A row describing the configuration of each slave RSU."
    INDEX   { rsuSetSlaveIndex }
    ::= { rsuSetSlaveTable 1 }

RsuSetSlaveEntry ::= SEQUENCE {
      rsuSetSlaveIndex              RsuTableIndex,
      rsuSetSlaveIpAddress          Ipv6Address,
      rsuSetSlaveRowStatus          RowStatus
}

rsuSetSlaveIndex OBJECT-TYPE
    SYNTAX       RsuTableIndex
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        " Slave RSU index "
    ::= { rsuSetSlaveEntry 1 }

rsuSetSlaveIpAddress OBJECT-TYPE
    SYNTAX       Ipv6Address
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "Contains the IPv6 address of each slave RSU. One
             slave per row."
    ::= { rsuSetSlaveEntry 2 }

rsuSetSlaveRowStatus OBJECT-TYPE
      SYNTAX       RowStatus
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION
        "create or destroy rows"
    ::= { rsuSetSlaveEntry 3 }


-- RSU Mode

rsuMode OBJECT-TYPE
    SYNTAX      INTEGER {
```

```
                    standby  (2),
                    operate  (4),
                    off      (16)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Specifies the current mode of operation of the RSU."
    ::= { rsuMIB 99 }


-- Asynchronous Messages
rsuAsync OBJECT IDENTIFIER ::= { rsuMIB 100 }

-- Notifications

rsuNotifications OBJECT IDENTIFIER ::= { rsuAsync 0 }


messageFileIntegrityError NOTIFICATION-TYPE
      OBJECTS      { rsuAlertLevel, rsuMsgFileIntegrityMsg }
      STATUS       current
      DESCRIPTION
            "The SNMP agent should immediately report integrity check
             errors on select store-and-forward messages to the SNMP
             manager."
      ::= { rsuNotifications 1 }

rsuSecStorageIntegrityError NOTIFICATION-TYPE
      OBJECTS      { rsuAlertLevel, rsuSecStorageIntegrityMsg }
      STATUS       current
      DESCRIPTION
            "The SNMP agent should immediately report integrity check
             errors in secure storage to the SNMP manager."
      ::= { rsuNotifications 2 }

rsuTamperAlert NOTIFICATION-TYPE
      OBJECTS      { rsuAlertLevel, rsuTamperAlertMsg }
      STATUS       current
      DESCRIPTION
            "The SNMP agent should report any tampering to the enclosure
             to the SNMP manager."
      ::= { rsuNotifications 3 }

rsuAuthError NOTIFICATION-TYPE
      OBJECTS      { rsuAlertLevel, rsuAuthMsg }
      STATUS       current
      DESCRIPTION
            "The SNMP agent should report an error in authorization
             to the SNMP manager."
      ::= { rsuNotifications 4 }

rsuSignatureVerifyError NOTIFICATION-TYPE
      OBJECTS      { rsuAlertLevel, rsuSignatureVerifyMsg }
```

```
      STATUS       current
      DESCRIPTION
            "The SNMP agent should report any signature verification errors
             to the SNMP manager."
      ::= { rsuNotifications 5 }

rsuAccessError NOTIFICATION-TYPE
      OBJECTS      { rsuAlertLevel, rsuAccessMsg }
      STATUS       current
      DESCRIPTION
            "The SNMP agent should report an access error or rejection due to
             a violation of the Access Control List."
      ::= { rsuNotifications 6 }

rsuTimeSourceLost NOTIFICATION-TYPE
      OBJECTS      { rsuAlertLevel, rsuTimeSourceLostMsg }
      STATUS       current
      DESCRIPTION
            "The SNMP agent should report to the SNMP manager that a
             time source was lost."
      ::= { rsuNotifications 7 }

rsuClockSkewError NOTIFICATION-TYPE
      OBJECTS      { rsuAlertLevel, rsuClockSkewMsg }
      STATUS       current
      DESCRIPTION
            "The SNMP agent should report to the SNMP manager a skew rate in
             the clock signal that exceeds a vendor-defined value."
      ::= { rsuNotifications 8 }

rsuTimeSourceMismatch NOTIFICATION-TYPE
      OBJECTS      { rsuAlertLevel, rsuTimeSourceMismatchMsg }
      STATUS       current
      DESCRIPTION
            "The SNMP agent should report to the SNMP manager a deviation
between
             two time sources that exceeds a vendor-defined threshold."
      ::= { rsuNotifications 9 }

rsuGpsAnomaly NOTIFICATION-TYPE
      OBJECTS      { rsuAlertLevel, rsuGpsAnomalyMsg }
      STATUS       current
      DESCRIPTION
            "The SNMP agent should report any anomalous GPS readings
             to the SNMP manager."
      ::= { rsuNotifications 10 }

rsuGpsDeviationError NOTIFICATION-TYPE
      OBJECTS      { rsuAlertLevel, rsuGpsDeviationMsg }
      STATUS       current
      DESCRIPTION
            "The SNMP agent should report to the SNMP manager a deviation in
             GPS position that is greater than the configured value."
      ::= { rsuNotifications 11 }
```

```
rsuGpsNmeaNotify NOTIFICATION-TYPE
      OBJECTS      { rsuAlertLevel, rsuGpsOutputString }
      STATUS       current
      DESCRIPTION
            "The SNMP agent should report the NMEA string to the SNMP manager
             at the configured interval."
      ::= { rsuNotifications 12 }


rsuNotificationObjects OBJECT IDENTIFIER ::= { rsuAsync 1 }

-- Notification Objects
rsuMsgFileIntegrityMsg OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "Contains the error message detailing an Active Message
             Integrity error "
      ::= { rsuNotificationObjects 1 }

rsuSecStorageIntegrityMsg OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "Contains the error message detailing a secure storage
             Integrity error "
      ::= { rsuNotificationObjects 2 }

rsuTamperAlertMsg OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "Contains the error message detailing an enclosure
             tampering error "
      ::= { rsuNotificationObjects 3 }

rsuAuthMsg OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "Contains the error message detailing an authorization error "
      ::= { rsuNotificationObjects 4 }

rsuSignatureVerifyMsg OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "Contains the error message detailing a signature verification
```

```
             error "
      ::= { rsuNotificationObjects 5 }

rsuAccessMsg OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "Contains the error message detailing an error or rejection
             due to Access Control List rules "
      ::= { rsuNotificationObjects 6 }

rsuTimeSourceLostMsg OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "Contains the error message indicating a time source
             was lost"
      ::= { rsuNotificationObjects 7 }

rsuClockSkewMsg OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "Contains the error message detailing that a vendor-defined
             clock skew rate was exceeded "
      ::= { rsuNotificationObjects 8 }

rsuTimeSourceMismatchMsg OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "Contains the error message detailing a deviation between
             two time sources that exceeds a vendor-defined threshold "
      ::= { rsuNotificationObjects 9 }

rsuGpsAnomalyMsg OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "Contains the error message detailing an anomaly that was
             detected in the GPS signal "
      ::= { rsuNotificationObjects 10 }

rsuGpsDeviationMsg OBJECT-TYPE
      SYNTAX       DisplayString
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "Contains the error message indicating that the reported GPS
```

```
              position differs from the reference by more than the
              allowed deviation "
      ::= { rsuNotificationObjects 11 }

rsuGpsNmeaNotifyInterval OBJECT-TYPE
      SYNTAX       Integer32 (0..18000)
      MAX-ACCESS   read-write
      STATUS       current
      DESCRIPTION
            "Sets the repeat interval in seconds for the Notification
             containing the GPS NMEA GPGGA string.
             Default is 0 (disabled)."
      ::= { rsuNotificationObjects 12 }

rsuAlertLevel OBJECT-TYPE
      SYNTAX       INTEGER {
                    info(0),
                          notice(1),
                          warning(2),
                          error(3),
                          critical(4)
                          }
      MAX-ACCESS   accessible-for-notify
      STATUS       current
      DESCRIPTION
            "The level of importance of the notification."
      ::= { rsuNotificationObjects 13 }

END
```

B.2. General MIB Objects

This section contains a list of MIB Objects for a typical Linux device. The RSU is expected to, at a minimum, support these or similar Objects with corresponding Object Identifiers.

```
sysDescr OBJECT-TYPE                    1.3.6.1.2.1.1.1
sysObjectID OBJECT-TYPE                 1.3.6.1.2.1.1.2
sysUpTime OBJECT-TYPE                   1.3.6.1.2.1.1.3
sysContact OBJECT-TYPE                  1.3.6.1.2.1.1.4
sysName OBJECT-TYPE                     1.3.6.1.2.1.1.5
sysLocation OBJECT-TYPE                 1.3.6.1.2.1.1.6
sysServices OBJECT-TYPE                 1.3.6.1.2.1.1.7
ifNumber OBJECT-TYPE                    1.3.6.1.2.1.2.1
ifTable OBJECT-TYPE                     1.3.6.1.2.1.2.2
ifEntry OBJECT-TYPE                     1.3.6.1.2.1.2.2.1
ifIndex OBJECT-TYPE                     1.3.6.1.2.1.2.2.1.1
ifDescr OBJECT-TYPE                     1.3.6.1.2.1.2.2.1.2
ifType OBJECT-TYPE                      1.3.6.1.2.1.2.2.1.3
ifMtu OBJECT-TYPE                       1.3.6.1.2.1.2.2.1.4
ifSpeed OBJECT-TYPE                     1.3.6.1.2.1.2.2.1.5
ifPhysAddress OBJECT-TYPE               1.3.6.1.2.1.2.2.1.6
ifAdminStatus OBJECT-TYPE               1.3.6.1.2.1.2.2.1.7
ifOperStatus OBJECT-TYPE                1.3.6.1.2.1.2.2.1.8
ifLastChange OBJECT-TYPE                1.3.6.1.2.1.2.2.1.9
ifInOctets OBJECT-TYPE                  1.3.6.1.2.1.2.2.1.10
ifInUcastPkts OBJECT-TYPE               1.3.6.1.2.1.2.2.1.11
ifInNUcastPkts OBJECT-TYPE              1.3.6.1.2.1.2.2.1.12
ifInDiscards OBJECT-TYPE                1.3.6.1.2.1.2.2.1.13
ifInErrors OBJECT-TYPE                  1.3.6.1.2.1.2.2.1.14
ifInUnknownProtos OBJECT-TYPE           1.3.6.1.2.1.2.2.1.15
ifOutOctets OBJECT-TYPE                 1.3.6.1.2.1.2.2.1.16
ifOutUcastPkts OBJECT-TYPE              1.3.6.1.2.1.2.2.1.17
ifOutNUcastPkts OBJECT-TYPE             1.3.6.1.2.1.2.2.1.18
ifOutDiscards OBJECT-TYPE               1.3.6.1.2.1.2.2.1.19
ifOutErrors OBJECT-TYPE                 1.3.6.1.2.1.2.2.1.20
ifOutQLen OBJECT-TYPE                   1.3.6.1.2.1.2.2.1.21
ifSpecific OBJECT-TYPE                  1.3.6.1.2.1.2.2.1.22
atTable OBJECT-TYPE                     1.3.6.1.2.1.3.1
atEntry OBJECT-TYPE                     1.3.6.1.2.1.3.1.1
atIfIndex OBJECT-TYPE                   1.3.6.1.2.1.3.1.1.1
atPhysAddress OBJECT-TYPE               1.3.6.1.2.1.3.1.1.2
```

```
atNetAddress OBJECT-TYPE                1.3.6.1.2.1.3.1.1.3
ipForwarding OBJECT-TYPE                1.3.6.1.2.1.4.1
ipDefaultTTL OBJECT-TYPE                1.3.6.1.2.1.4.2
ipInReceives OBJECT-TYPE                1.3.6.1.2.1.4.3
ipInHdrErrors OBJECT-TYPE               1.3.6.1.2.1.4.4
ipInAddrErrors OBJECT-TYPE              1.3.6.1.2.1.4.5
ipForwDatagrams OBJECT-TYPE             1.3.6.1.2.1.4.6
ipInUnknownProtos OBJECT-TYPE           1.3.6.1.2.1.4.7
ipInDiscards OBJECT-TYPE                1.3.6.1.2.1.4.8
ipInDelivers OBJECT-TYPE                1.3.6.1.2.1.4.9
ipOutRequests OBJECT-TYPE               1.3.6.1.2.1.4.10
ipOutDiscards OBJECT-TYPE               1.3.6.1.2.1.4.11
ipOutNoRoutes OBJECT-TYPE               1.3.6.1.2.1.4.12
ipReasmTimeout OBJECT-TYPE              1.3.6.1.2.1.4.13
ipReasmReqds OBJECT-TYPE                1.3.6.1.2.1.4.14
ipReasmOKs OBJECT-TYPE                  1.3.6.1.2.1.4.15
ipReasmFails OBJECT-TYPE                1.3.6.1.2.1.4.16
ipFragOKs OBJECT-TYPE                   1.3.6.1.2.1.4.18
ipFragFails OBJECT-TYPE                 1.3.6.1.2.1.4.18
ipFragCreates OBJECT-TYPE               1.3.6.1.2.1.4.19
ipAddrTable OBJECT-TYPE                 1.3.6.1.2.1.4.20
ipAddrEntry OBJECT-TYPE                 1.3.6.1.2.1.4.20.1
ipAdEntAddr OBJECT-TYPE                 1.3.6.1.2.1.4.20.1.1
ipAdEntIfIndex OBJECT-TYPE              1.3.6.1.2.1.4.20.1.2
ipAdEntNetMask OBJECT-TYPE              1.3.6.1.2.1.4.20.1.3
ipAdEntBcastAddr OBJECT-TYPE            1.3.6.1.2.1.4.20.1.4
ipAdEntReasmMaxSize OBJECT-TYPE         1.3.6.1.2.1.4.20.1.5
ipRouteTable OBJECT-TYPE                1.3.6.1.2.1.4.21
ipRouteEntry OBJECT-TYPE                1.3.6.1.2.1.4.21.1
ipRouteDest OBJECT-TYPE                 1.3.6.1.2.1.4.21.1.1
ipRouteIfIndex OBJECT-TYPE              1.3.6.1.2.1.4.21.1.2
ipRouteMetric1 OBJECT-TYPE              1.3.6.1.2.1.4.21.1.3
ipRouteMetric2 OBJECT-TYPE              1.3.6.1.2.1.4.21.1.4
ipRouteMetric3 OBJECT-TYPE              1.3.6.1.2.1.4.21.1.5
ipRouteMetric4 OBJECT-TYPE              1.3.6.1.2.1.4.21.1.6
ipRouteNextHop OBJECT-TYPE              1.3.6.1.2.1.4.21.1.7
ipRouteType OBJECT-TYPE                 1.3.6.1.2.1.4.21.1.8
ipRouteProto OBJECT-TYPE                1.3.6.1.2.1.4.21.1.9
ipRouteAge OBJECT-TYPE                  1.3.6.1.2.1.4.21.1.10
ipRouteMask OBJECT-TYPE                 1.3.6.1.2.1.4.21.1.11
ipRouteMetric5 OBJECT-TYPE              1.3.6.1.2.1.4.21.1.12
```

```
ipRouteInfo OBJECT-TYPE                 1.3.6.1.2.1.4.21.1.13
ipNetToMediaTable OBJECT-TYPE           1.3.6.1.2.1.4.22
ipNetToMediaEntry OBJECT-TYPE           1.3.6.1.2.1.4.22.1
ipNetToMediaIfIndex OBJECT-TYPE         1.3.6.1.2.1.4.22.1.1
ipNetToMediaPhysAddress OBJECT-TYPE     1.3.6.1.2.1.4.22.1.2
ipNetToMediaNetAddress OBJECT-TYPE      1.3.6.1.2.1.4.22.1.3
ipNetToMediaType OBJECT-TYPE            1.3.6.1.2.1.4.22.1.4
ipRoutingDiscards OBJECT-TYPE           1.3.6.1.2.1.4.23
icmpInMsgs OBJECT-TYPE                  1.3.6.1.2.1.5.1
icmpInErrors OBJECT-TYPE                1.3.6.1.2.1.5.2
icmpInDestUnreachs OBJECT-TYPE          1.3.6.1.2.1.5.3
icmpInTimeExcds OBJECT-TYPE             1.3.6.1.2.1.5.4
icmpInParmProbs OBJECT-TYPE             1.3.6.1.2.1.5.5
icmpInSrcQuenchs OBJECT-TYPE            1.3.6.1.2.1.5.6
icmpInRedirects OBJECT-TYPE             1.3.6.1.2.1.5.7
icmpInEchos OBJECT-TYPE                 1.3.6.1.2.1.5.8
icmpInEchoReps OBJECT-TYPE              1.3.6.1.2.1.5.9
icmpInTimestamps OBJECT-TYPE            1.3.6.1.2.1.5.10
icmpInTimestampReps OBJECT-TYPE         1.3.6.1.2.1.5.11
icmpInAddrMasks OBJECT-TYPE             1.3.6.1.2.1.5.12
icmpInAddrMaskReps OBJECT-TYPE          1.3.6.1.2.1.5.13
icmpOutMsgs OBJECT-TYPE                 1.3.6.1.2.1.5.14
icmpOutErrors OBJECT-TYPE               1.3.6.1.2.1.5.15
icmpOutDestUnreachs OBJECT-TYPE         1.3.6.1.2.1.5.16
icmpOutTimeExcds OBJECT-TYPE            1.3.6.1.2.1.5.17
icmpOutParmProbs OBJECT-TYPE            1.3.6.1.2.1.5.18
icmpOutSrcQuenchs OBJECT-TYPE           1.3.6.1.2.1.5.19
icmpOutRedirects OBJECT-TYPE            1.3.6.1.2.1.5.20
icmpOutEchos OBJECT-TYPE                1.3.6.1.2.1.5.21
icmpOutEchoReps OBJECT-TYPE             1.3.6.1.2.1.5.22
icmpOutTimestamps OBJECT-TYPE           1.3.6.1.2.1.5.23
icmpOutTimestampReps OBJECT-TYPE        1.3.6.1.2.1.5.24
icmpOutAddrMasks OBJECT-TYPE            1.3.6.1.2.1.5.25
icmpOutAddrMaskReps OBJECT-TYPE         1.3.6.1.2.1.5.26
tcpRtoAlgorithm OBJECT-TYPE             1.3.6.1.2.1.6.1
tcpRtoMin OBJECT-TYPE                   1.3.6.1.2.1.6.2
tcpRtoMax OBJECT-TYPE                   1.3.6.1.2.1.6.3
tcpMaxConn OBJECT-TYPE                  1.3.6.1.2.1.6.4
tcpActiveOpens OBJECT-TYPE              1.3.6.1.2.1.6.5
tcpPassiveOpens OBJECT-TYPE             1.3.6.1.2.1.6.6
tcpAttemptFails OBJECT-TYPE             1.3.6.1.2.1.6.7
```

```
tcpEstabResets OBJECT-TYPE              1.3.6.1.2.1.6.8
tcpCurrEstab OBJECT-TYPE                1.3.6.1.2.1.6.9
tcpInSegs OBJECT-TYPE                   1.3.6.1.2.1.6.10
tcpOutSegs OBJECT-TYPE                  1.3.6.1.2.1.6.11
tcpRetransSegs OBJECT-TYPE              1.3.6.1.2.1.6.12
the TCP Connection table                1.3.6.1.2.1.6.13
tcpConnEntry OBJECT-TYPE                1.3.6.1.2.1.6.13.1
tcpConnState OBJECT-TYPE                1.3.6.1.2.1.6.13.1.1
tcpConnLocalAddress OBJECT-TYPE         1.3.6.1.2.1.6.13.1.2
tcpConnLocalPort OBJECT-TYPE            1.3.6.1.2.1.6.13.1.3
tcpConnRemAddress OBJECT-TYPE           1.3.6.1.2.1.6.13.1.4
tcpConnRemPort OBJECT-TYPE              1.3.6.1.2.1.6.13.1.5
tcpInErrs OBJECT-TYPE                   1.3.6.1.2.1.6.14
tcpOutRsts OBJECT-TYPE                  1.3.6.1.2.1.6.15
udpInDatagrams OBJECT-TYPE              1.3.6.1.2.1.7.1
udpNoPorts OBJECT-TYPE                  1.3.6.1.2.1.7.2
udpInErrors OBJECT-TYPE                 1.3.6.1.2.1.7.3
udpOutDatagrams OBJECT-TYPE             1.3.6.1.2.1.7.4
udpTable OBJECT-TYPE                    1.3.6.1.2.1.7.5
udpEntry OBJECT-TYPE                    1.3.6.1.2.1.7.5.1
udpLocalAddress OBJECT-TYPE             1.3.6.1.2.1.7.5.1.1
udpLocalPort OBJECT-TYPE                1.3.6.1.2.1.7.5.1.2
egpInMsgs OBJECT-TYPE                   1.3.6.1.2.1.8.1
egpInErrors OBJECT-TYPE                 1.3.6.1.2.1.8.2
egpOutMsgs OBJECT-TYPE                  1.3.6.1.2.1.8.3
egpOutErrors OBJECT-TYPE                1.3.6.1.2.1.8.4
egpNeighTable OBJECT-TYPE               1.3.6.1.2.1.8.5
egpNeighEntry OBJECT-TYPE               1.3.6.1.2.1.8.5.1
egpNeighState OBJECT-TYPE               1.3.6.1.2.1.8.5.1.1
egpNeighAddr OBJECT-TYPE                1.3.6.1.2.1.8.5.1.2
egpNeighAs OBJECT-TYPE                  1.3.6.1.2.1.8.5.1.3
egpNeighInMsgs OBJECT-TYPE              1.3.6.1.2.1.8.5.1.4
egpNeighInErrs OBJECT-TYPE              1.3.6.1.2.1.8.5.1.5
egpNeighOutMsgs OBJECT-TYPE             1.3.6.1.2.1.8.5.1.6
egpNeighOutErrs OBJECT-TYPE             1.3.6.1.2.1.8.5.1.7
egpNeighInErrMsgs OBJECT-TYPE           1.3.6.1.2.1.8.5.1.8
egpNeighOutErrMsgs OBJECT-TYPE          1.3.6.1.2.1.8.5.1.9
egpNeighStateUps OBJECT-TYPE            1.3.6.1.2.1.8.5.1.10
egpNeighStateDowns OBJECT-TYPE          1.3.6.1.2.1.8.5.1.11
egpNeighIntervalHello OBJECT-TYPE       1.3.6.1.2.1.8.5.1.12
egpNeighIntervalPoll OBJECT-TYPE        1.3.6.1.2.1.8.5.1.13
```

```
egpNeighMode OBJECT-TYPE                1.3.6.1.2.1.8.5.1.14
egpNeighEventTrigger OBJECT-TYPE        1.3.6.1.2.1.8.5.1.15
egpAs OBJECT-TYPE                       1.3.6.1.2.1.8.6
the Transmission group                  1.3.6.1.2.1.10
the SNMP group                          1.3.6.1.2.1.11
snmpInPkts OBJECT-TYPE                  1.3.6.1.2.1.11.1
snmpOutPkts OBJECT-TYPE                 1.3.6.1.2.1.11.2
snmpInBadVersions OBJECT-TYPE           1.3.6.1.2.1.11.3
snmpInBadCommunityNames OBJECT-TYPE     1.3.6.1.2.1.11.4
snmpInBadCommunityUses OBJECT-TYPE      1.3.6.1.2.1.11.5
snmpInASNParseErrs OBJECT-TYPE          1.3.6.1.2.1.11.6
snmpInTooBigs OBJECT-TYPE               1.3.6.1.2.1.11.8
snmpInNoSuchNames OBJECT-TYPE           1.3.6.1.2.1.11.9
snmpInBadValues OBJECT-TYPE             1.3.6.1.2.1.11.10
snmpInReadOnlys OBJECT-TYPE             1.3.6.1.2.1.11.11
snmpInGenErrs OBJECT-TYPE               1.3.6.1.2.1.11.12
snmpInTotalReqVars OBJECT-TYPE          1.3.6.1.2.1.11.13
snmpInTotalSetVars OBJECT-TYPE          1.3.6.1.2.1.11.14
snmpInGetRequests OBJECT-TYPE           1.3.6.1.2.1.11.15
snmpInGetNexts OBJECT-TYPE              1.3.6.1.2.1.11.16
snmpInSetRequests OBJECT-TYPE           1.3.6.1.2.1.11.17
snmpInGetResponses OBJECT-TYPE          1.3.6.1.2.1.11.18
snmpInTraps OBJECT-TYPE                 1.3.6.1.2.1.11.19
snmpOutTooBigs OBJECT-TYPE              1.3.6.1.2.1.11.20
snmpOutNoSuchNames OBJECT-TYPE          1.3.6.1.2.1.11.21
snmpOutBadValues OBJECT-TYPE            1.3.6.1.2.1.11.22
snmpOutGenErrs OBJECT-TYPE              1.3.6.1.2.1.11.24
snmpOutGetRequests OBJECT-TYPE          1.3.6.1.2.1.11.25
snmpOutGetNexts OBJECT-TYPE             1.3.6.1.2.1.11.26
snmpOutSetRequests OBJECT-TYPE          1.3.6.1.2.1.11.27
snmpOutGetResponses OBJECT-TYPE         1.3.6.1.2.1.11.28
snmpOutTraps OBJECT-TYPE                1.3.6.1.2.1.11.29
snmpEnableAuthenTraps OBJECT-TYPE       1.3.6.1.2.1.11.30
```

B.3. IPv6 MIB Objects

This section contains a list of IPv6 MIB Objects for a typical Linux device. The RSU is expected to, at a minimum, support these, or similar Objects with corresponding Object Identities.

```
ipv6Forwarding OBJECT-TYPE                    1.3.6.1.2.1.55.1.1.0
```

```
ipv6DefaultHopLimit OBJECT-TYPE                 1.3.6.1.2.1.55.1.2.0
ipv6Interfaces OBJECT-TYPE                      1.3.6.1.2.1.55.1.3.0
ipv6IfTableLastChange OBJECT-TYPE               1.3.6.1.2.1.55.1.4.0
ipv6IfTable OBJECT-TYPE                         1.3.6.1.2.1.55.1.5
ipv6IfEntry OBJECT-TYPE                         1.3.6.1.2.1.55.1.5.1
ipv6IfIndex OBJECT-TYPE                         1.3.6.1.2.1.55.1.5.1.1
ipv6IfDescr OBJECT-TYPE                         1.3.6.1.2.1.55.1.5.1.2
ipv6IfLowerLayer OBJECT-TYPE                    1.3.6.1.2.1.55.1.5.1.3
ipv6IfEffectiveMtu OBJECT-TYPE                  1.3.6.1.2.1.55.1.5.1.4
ipv6IfReasmMaxSize OBJECT-TYPE                  1.3.6.1.2.1.55.1.5.1.5
ipv6IfIdentifier OBJECT-TYPE                    1.3.6.1.2.1.55.1.5.1.6
ipv6IfIdentifierLength OBJECT-TYPE              1.3.6.1.2.1.55.1.5.1.7
ipv6IfPhysicalAddress OBJECT-TYPE               1.3.6.1.2.1.55.1.5.1.8
ipv6IfAdminStatus OBJECT-TYPE                   1.3.6.1.2.1.55.1.5.1.9
ipv6IfOperStatus OBJECT-TYPE                    1.3.6.1.2.1.55.1.10
ipv6IfLastChange OBJECT-TYPE                    1.3.6.1.2.1.55.1.5.11
ipv6IfStatsTable OBJECT-TYPE                    1.3.6.1.2.1.55.1.6
ipv6IfStatsEntry OBJECT-TYPE                    1.3.6.1.2.1.55.1.6.1
ipv6IfStatsInReceives OBJECT-TYPE               1.3.6.1.2.1.55.1.6.1.1
ipv6IfStatsInHdrErrors OBJECT-TYPE              1.3.6.1.2.1.55.1.6.1.2
ipv6IfStatsInTooBigErrors OBJECT-TYPE           1.3.6.1.2.1.55.1.6.1.3
ipv6IfStatsInNoRoutes OBJECT-TYPE               1.3.6.1.2.1.55.1.6.1.4
ipv6IfStatsInAddrErrors OBJECT-TYPE             1.3.6.1.2.1.55.1.6.1.5
ipv6IfStatsInUnknownProtos OBJECT-TYPE          1.3.6.1.2.1.55.1.6.1.6
ipv6IfStatsInTruncatedPkts OBJECT-TYPE          1.3.6.1.2.1.55.1.6.1.7
ipv6IfStatsInDiscards OBJECT-TYPE               1.3.6.1.2.1.55.1.6.1.8
ipv6IfStatsInDelivers OBJECT-TYPE               1.3.6.1.2.1.55.1.6.1.9
ipv6IfStatsOutForwDatagrams OBJECT-TYPE         1.3.6.1.2.1.55.1.6.1.10
ipv6IfStatsOutRequests OBJECT-TYPE              1.3.6.1.2.1.55.1.6.1.11
ipv6IfStatsOutDiscards OBJECT-TYPE              1.3.6.1.2.1.55.1.6.1.12
ipv6IfStatsOutFragOKs OBJECT-TYPE               1.3.6.1.2.1.55.1.6.1.13
ipv6IfStatsOutFragFails OBJECT-TYPE             1.3.6.1.2.1.55.1.6.1.14
ipv6IfStatsOutFragCreates OBJECT-TYPE           1.3.6.1.2.1.55.1.6.1.15
ipv6IfStatsReasmReqds OBJECT-TYPE               1.3.6.1.2.1.55.1.6.1.16
ipv6IfStatsReasmOKs OBJECT-TYPE                 1.3.6.1.2.1.55.1.6.1.17
ipv6IfStatsReasmFails OBJECT-TYPE               1.3.6.1.2.1.55.1.6.1.18
ipv6IfStatsInMcastPkts OBJECT-TYPE              1.3.6.1.2.1.55.1.6.1.19
ipv6IfStatsOutMcastPkts OBJECT-TYPE             1.3.6.1.2.1.55.1.6.1.20
ipv6AddrPrefixTable OBJECT-TYPE                 1.3.6.1.2.1.55.1.7.0.0
ipv6AddrPrefixEntry OBJECT-TYPE                 1.3.6.1.2.1.55.1.7.1
ipv6AddrPrefix OBJECT-TYPE                      1.3.6.1.2.1.55.1.7.1.1
```

```
ipv6AddrPrefixLength OBJECT-TYPE                    1.3.6.1.2.1.55.1.7.1.2
ipv6AddrPrefixOnLinkFlag OBJECT-TYPE                1.3.6.1.2.1.55.1.7.1.3
ipv6AddrPrefixAutonomousFlag OBJECT-TYPE            1.3.6.1.2.1.55.1.7.1.4
ipv6AddrPrefixAdvPreferredLifetime OBJECT-TYPE      1.3.6.1.2.1.55.1.7.1.5
ipv6AddrPrefixAdvValidLifetime OBJECT-TYPE          1.3.6.1.2.1.55.1.7.1.6
ipv6AddrTable OBJECT-TYPE                           1.3.6.1.2.1.55.1.8
ipv6AddrEntry OBJECT-TYPE                           1.3.6.1.2.1.55.1.8.1
ipv6AddrAddress OBJECT-TYPE                         1.3.6.1.2.1.55.1.8.1.1
ipv6AddrPfxLength OBJECT-TYPE                       1.3.6.1.2.1.55.1.8.1.2
ipv6AddrType OBJECT-TYPE                            1.3.6.1.2.1.55.1.8.1.3
ipv6AddrAnycastFlag OBJECT-TYPE                     1.3.6.1.2.1.55.1.8.1.4
ipv6AddrStatus OBJECT-TYPE                          1.3.6.1.2.1.55.1.8.1.5
ipv6RouteNumber OBJECT-TYPE                         1.3.6.1.2.1.55.1.9.0
ipv6DiscardedRoutes OBJECT-TYPE                     1.3.6.1.2.1.55.1.10.0
ipv6RouteTable OBJECT-TYPE                          1.3.6.1.2.1.55.1.11.0
ipv6RouteEntry OBJECT-TYPE                          1.3.6.1.2.1.55.1.11.1.0
ipv6RouteDest OBJECT-TYPE                           1.3.6.1.2.1.55.1.11.1.1
ipv6RoutePfxLength OBJECT-TYPE                      1.3.6.1.2.1.55.1.11.1.2
ipv6RouteIndex OBJECT-TYPE                          1.3.6.1.2.1.55.1.11.1.3
ipv6RouteIfIndex OBJECT-TYPE                        1.3.6.1.2.1.55.1.11.1.4
ipv6RouteNextHop OBJECT-TYPE                        1.3.6.1.2.1.55.1.11.1.5
ipv6RouteType OBJECT-TYPE                           1.3.6.1.2.1.55.1.11.1.6
ipv6RouteProtocol OBJECT-TYPE                       1.3.6.1.2.1.55.1.11.1.7
ipv6RoutePolicy OBJECT-TYPE                         1.3.6.1.2.1.55.1.11.1.8
ipv6RouteAge OBJECT-TYPE                            1.3.6.1.2.1.55.1.11.1.9
ipv6RouteNextHopRDI OBJECT-TYPE                     1.3.6.1.2.1.55.1.11.1.10
ipv6RouteMetric OBJECT-TYPE                         1.3.6.1.2.1.55.1.11.1.11
ipv6RouteWeight OBJECT-TYPE                         1.3.6.1.2.1.55.1.11.1.12
ipv6RouteInfo OBJECT-TYPE                           1.3.6.1.2.1.55.1.11.1.13
ipv6RouteValid OBJECT-TYPE                          1.3.6.1.2.1.55.1.11.1.14
ipv6NetToMediaTable OBJECT-TYPE                     1.3.6.1.2.1.55.1.12.0
ipv6NetToMediaEntry OBJECT-TYPE                     1.3.6.1.2.1.55.1.12.1.0
ipv6NetToMediaNetAddress OBJECT-TYPE                1.3.6.1.2.1.55.1.12.1.1
ipv6NetToMediaPhysAddress OBJECT-TYPE               1.3.6.1.2.1.55.1.12.1.2
ipv6NetToMediaType OBJECT-TYPE                      1.3.6.1.2.1.55.1.12.1.3
ipv6IfNetToMediaState OBJECT-TYPE                   1.3.6.1.2.1.55.1.12.1.4
ipv6IfNetToMediaLastUpdated OBJECT-TYPE             1.3.6.1.2.1.55.1.12.1.5
ipv6NetToMediaValid OBJECT-TYPE                     1.3.6.1.2.1.55.1.12.1.6
ipv6Notifications      OBJECT IDENTIFIER            1.3.6.1.2.1.55.2
ipv6NotificationPrefix OBJECT IDENTIFIER            1.3.6.1.2.1.55.2.0
ipv6IfStateChange NOTIFICATION-TYPE                 1.3.6.1.2.1.55.2.0.1
```

```
ipv6Conformance OBJECT IDENTIFIER                1.3.6.1.2.1.55.3
ipv6Compliances OBJECT IDENTIFIER                1.3.6.1.2.1.55.3.1
ipv6Groups      OBJECT IDENTIFIER                1.3.6.1.2.1.55.3.2
ipv6Compliance MODULE-COMPLIANCE                 1.3.6.1.2.1.55.3.2.1
```

B.4. RSU Specific MIB Object Map

This section contains a mapping of the RSU specific MIB OIDs from section 0 above.

Name	OID 15628.4.x	Max-Access	Syntax	Range
Continuous MAC Address				
rsuContMacAddress	1.1	read-only	MacAddress	
Alternating Mac Address				
rsuAltMacAddress	1.2	read-only	MacAddress	
GPS Status				
rsuGPSStatus	1.3	read-only	Integer32	0..15
Store and Repeat				
rsuSRMStatusTable	1.4	not-accessible	SEQUENCE OF	
rsuSRMStatusEntry	1.4.1	not-accessible	RsuSRMStatusEntry	
rsuSRMIndex	1.4.1.1	not-accessible	RsuTableIndex	
rsuSRMPsid	1.4.1.2	read-create	RsuPsidTC	
rsuSRMDsrcMsgId	1.4.1.3	read-create	Integer32	
rsuSRMTxMode	1.4.1.4	read-create	INTEGER	0|1
rsuSRMTxChannel	1.4.1.5	read-create	Integer32	172..184
rsuSRMTxInterval	1.4.1.6	read-create	Integer32	1..2147483647
rsuSRMDeliveryStart	1.4.1.7	read-create	OCTET STRING	SIZE(0|6)
rsuSRMDeliveryStop	1.4.1.8	read-create	OCTET STRING	SIZE(0|6)
rsuSRMPayload	1.4.1.9	read-create	OCTET STRING	SIZE(0..1500)
rsuSRMEnable	1.4.1.10	read-create	INTEGER	0|1
rsuSRMStatus	1.4.1.11	read-create	RowStatus	
Immediate Forward				
rsuIFMStatusTable	1.5	not-accessible	SEQUENCE OF	
rsuIFMStatusEntry	1.5.1	not-accessible	RsuIFMStatusEntry	

Name	OID 15628.4.x	Max-Access	Syntax	Range
rsuIFMIndex	1.5.1.1	not-accessible	RsuTableIndex	
rsuIFMPsid	1.5.1.2	read-create	RsuPsidTC	
rsuIFMDsrcMsgId	1.5.1.3	read-create	Integer32	
rsuIFMTxMode	1.5.1.4	read-create	INTEGER	0|1
rsuIFMTxChannel	1.5.1.5	read-create	Integer32	172..184
rsuIFMEnable	1.5.1.6	read-create	INTEGER	0|1
rsuIFMStatus	1.5.1.7	read-create	RowStatus	
Device ID				
rsuSysObjectID	1.6	read-only	OBJECT IDENTIFIER	
DSRC Forwarding				
rsuDsrcForwardTable	1.7	not-accessible	SEQUENCE OF	
rsuDsrcForwardEntry	1.7.1	not-accessible	RsuDsrcForwardEntry	
rsuDsrcForwardIndex	1.7.1.1	not-accessible	RsuTableIndex	
rsuDsrcFwdPsid	1.7.1.2	read-create	RsuPsidTC	
rsuDsrcFwdDestIPAddr	1.7.1.3	read-create	Ipv6Address	
rsuDsrcFwdDestPort	1.7.1.4	read-create	Integer32	1024..65535
rsuDsrcFwdProtocol	1.7.1.5	read-create	INTEGER	1|2
rsuDsrcFwdRssi	1.7.1.6	read-create	Integer32	-100..-60
rsuDsrcFwdMsgInterval	1.7.1.7	read-create	Integer32	1..9
rsuDsrcFwdDeliveryStart	1.7.1.8	read-create	OCTET STRING	SIZE(0|6)
rsuDsrcFwdDeliveryStop	1.7.1.9	read-create	OCTET STRING	SIZE(0|6)
rsuDsrcFwdEnable	1.7.1.10	read-create	INTEGER	0|1
messageForwardingRowStatus	1.7.1.11	read-create	RowStatus	
GPS Config				
rsuGpsOutput	1.8			
rsuGpsOutputPort	1.8.1	read-write	Integer32	1024..65535
rsuGpsOutputAddress	1.8.2	read-write	Ipv6Address	

Name	OID 15628.4.x	Max-Access	Syntax	Range
rsuGpsOutputInterface	1.8.3	read-write	DisplayString	
rsuGpsOutputInterval	1.8.4	read-write	Integer32	1..18000
rsuGpsOutputString	1.8.5	read-only	DisplayString	SIZE(0..100)
rsuGpsRefLat	1.8.6	read-write	Integer32	-900000000..900000000
rsuGpsRefLon	1.8.7	read-write	Integer32	-1800000000..1800000000
rsuGpsRefElv	1.8.8	read-write	Integer32	-100000..1000000
rsuGpsMaxDeviation	1.8.9	read-write	Integer32	1..2000000
Interface Logging Config				
rsuInterfaceLogTable	1.9	not-accessible	SEQUENCE OF	
rsuInterfaceLogEntry	1.9.1	not-accessible	RsuInterfaceLogEntry	
rsuIfaceLogIndex	1.9.1.1	not-accessible	RsuTableIndex	
rsuIfaceGenerate	1.9.1.2	read-write	INTEGER	0|1
rsuIfaceMaxFileSize	1.9.1.3	read-write	Integer32	5..40
rsuIfaceMaxFileTime	1.9.1.4	read-write	Integer32	1..48
rsuIfaceLogByDir	1.9.1.5	read-write	INTEGER	0|1
rsuIfaceName	1.9.1.6	read-only	DisplayString	
Cert requests				
rsuSecCredReq	1.10	read-write	OCTET STRING	SIZE(1)
1609.2 Config				
rsuSecCredAttachInterval	1.11	read-write	INTEGER	1..100
DSRC Interface Config				
rsuDsrcChannelModeTable	1.12	not-accessible	SEQUENCE OF	
rsuDsrcChannelModeEntry	1.12.1	not-accessible	RsuDsrcChannelModeEntry	
rsuDCMIndex	1.12.1.1	not-accessible	RsuTableIndex	
rsuDCMRadio	1.12.1.2	read-only	DisplayString	
rsuDCMMode	1.12.1.3	read-write	INTEGER	0|1
rsuDCMCCH	1.12.1.4	read-write	Integer32	172..184

Name	OID 15628.4.x	Max-Access	Syntax	Range
rsuDCMSCH	1.12.1.5	read-write	Integer32	172..184
WSA Message Config				
rsuWsaServiceTable	1.13	not-accessible	SEQUENCE OF	
rsuWsaServiceEntry	1.13.1	not-accessible	RsuWsaServiceEntry	
rsuWsaIndex	1.13.1.1	not-accessible	RsuTableIndex	
rsuWsaPsid	1.13.1.2	read-create	RsuPsidTC	
rsuWsaPriority	1.13.1.3	read-create	INTEGER	0..63
rsuWsaProviderContext	1.13.1.4	read-create	DisplayString	SIZE(4)
rsuWsaIpAddress	1.13.1.5	read-create	Ipv6Address	
rsuWsaPort	1.13.1.6	read-create	Integer32	1024..65535
rsuWsaChannel	1.13.1.7	read-create	Integer32	172..184
rsuWsaStatus	1.13.1.8	read-create	RowStatus	
WRA Config				
rsuWraConfiguration	1.14			
rsuWraIpPrefix	1.14.1	read-write	Ipv6Address	
rsuWraIpPrefixLength	1.14.2	read-write	OCTET STRING	SIZE(1)
rsuWraGateway	1.14.3	read-write	Ipv6Address	
rsuWraPrimaryDns	1.14.4	read-write	Ipv6Address	
Message Statistics				
rsuMessageStats	1.15			
rsuAltSchMsgSent	1.15.1	read-only	Counter32	0-2^32
rsuAltSchMsgRcvd	1.15.2	read-only	Counter32	0-2^32
rsuAltCchMsgSent	1.15.3	read-only	Counter32	0-2^32
rsuAltCchMsgRcvd	1.15.4	read-only	Counter32	0-2^32
rsuContSchMsgSent	1.15.5	read-only	Counter32	0-2^32
rsuContSchMsgRcvd	1.15.6	read-only	Counter32	0-2^32
rsuContCchMsgSent	1.15.7	read-only	Counter32	0-2^32

Name	OID 15628.4.x	Max-Access	Syntax	Range
rsuContCchMsgRcvd	1.15.8	read-only	Counter32	0-2^32
rsuMessageCountsByPsidTable	1.15.9	not-accessible	SEQUENCE OF	
rsuMessageCountsByPsidEntry	1.15.9.1	not-accessible	RsuMessageCountsByPsidEntry	
rsuMessageCountsByPsidIndex	1.15.9.1.1	not-accessible	RsuTableIndex	
rsuMessageCountsByPsidId	1.15.9.1.2	read-create	RsuPsidTC	
rsuMessageCountsByPsidCounts	1.15.9.1.3	read-create	Counter32	0-2^32
rsuMessageCountsByPsidRowStatus	1.15.9.1.4	read-create	RowStatus	
System Statistics				
rsuSystemStats	1.16			
rsuTimeSincePowerOn	1.16.1	read-only	Counter32	0-2^32 sec
rsuTotalRunTime	1.16.2	read-only	Counter32	0-2^32 sec
rsuLastLoginTime	1.16.3	read-only	DateAndTime	
rsuLastLoginUser	1.16.4	read-only	DisplayString	SIZE(0..32)
rsuLastLoginSource	1.16.5	read-only	DisplayString	SIZE(0..32)
rsuLastRestartTime	1.16.6	read-only	DateAndTime	
rsuIntTemp	1.16.7	read-only	Integer32	-100..100
System Description				
rsuSysDescription	1.17			
rsuMibVersion	1.17.1	read-only	DisplayString	SIZE(0..32)
rsuFirmwareVersion	1.17.2	read-only	DisplayString	SIZE(0..32)
rsuLocationDesc	1.17.3	read-write	DisplayString	SIZE(0..140)
rsuId	1.17.4	read-write	DisplayString	SIZE(0..32)
rsuManufacturer	1.17.5	read-only	DisplayString	SIZE(0..32)
System Settings				
rsuSysSettings	1.18			
rsuTxPower	1.18.1	read-write	Integer32	0..100
rsuNotifyIpAddress	1.18.2	read-write	Ipv6Address	

Name	OID 15628.4.x	Max-Access	Syntax	Range
rsuNotifyPort	1.18.3	read-write	Integer32	0..65535
rsuSysLogCloseDay	1.18.4	read-write	INTEGER	1..7
rsuSysLogCloseTime	1.18.5	read-write	OCTET STRING	SIZE(3)
rsuSysLogDeleteDay	1.18.6	read-write	INTEGER	1..7
rsuSysLogDeleteAge	1.18.7	read-write	Integer32	
System Status				
rsuChanStatus	1.19.1	read-only	INTEGER	0..3
Situation Data				
rsuSitData	1.20			
rsuSdcDestIpAddress	1.20.1	read-write	Ipv6Address	
rsuSdcDestPort	1.20.2	read-write	Integer32	1024..65535
rsuSdcInterval	1.20.3	read-write	Integer32	1..18000
rsuSdwIpAddress	1.20.4	read-write	Ipv6Address	
rsuSdwPort	1.20.5	read-write	Integer32	1024..65535
RSU Set				
rsuSet	1.21			
rsuSetRole	1.21.1	read-write	INTEGER	0|1
rsuSetEnable	1.21.2	read-write	INTEGER	0|1
rsuSetSlaveTable	1.21.3	not-accessible	SEQUENCE OF	
rsuSetSlaveEntry	1.21.3.1	not-accessible	RsuSetSlaveEntry	
rsuSetSlaveIndex	1.21.3.1.1	not-accessible	RsuTableIndex	
rsuSetSlaveIpAddress	1.21.3.1.2	read-create	Ipv6Address	
rsuSetSlaveRowStatus	1.21.3.1.3	read-create	RowStatus	
Mode				
rsuMode	1.99	read-write	INTEGER	2|4|16
Notifications				
rsuMsgFileIntegrityError	1.100.0.1		NOTIFICATION-TYPE	

Name	OID 15628.4.x	Max-Access	Syntax	Range
rsuSecStorageIntegrityError	1.100.0.2		NOTIFICATION-TYPE	
rsuTamperAlert	1.100.0.3		NOTIFICATION-TYPE	
rsuAuthError	1.100.0.4		NOTIFICATION-TYPE	
rsuSignatureVerifyError	1.100.0.5		NOTIFICATION-TYPE	
rsuAccessError	1.100.0.6		NOTIFICATION-TYPE	
rsuTimeSourceLost	1.100.0.7		NOTIFICATION-TYPE	
rsuClockSkewError	1.100.0.8		NOTIFICATION-TYPE	
rsuTimeSourceMismatch	1.100.0.9		NOTIFICATION-TYPE	
rsuGpsAnomaly	1.100.0.10		NOTIFICATION-TYPE	
rsuGpsDeviationError	1.100.0.11		NOTIFICATION-TYPE	
rsuGpsNmeaNotify	1.100.0.12		NOTIFICATION-TYPE	
Notification Objects				
rsuMsgFileIntegrityMsg	1.100.1.1	accessible-for-notify	DisplayString	
rsuSecStorageIntegrityMsg	1.100.1.2	accessible-for-notify	DisplayString	
rsuTamperAlertMsg	1.100.1.3	accessible-for-notify	DisplayString	
rsuAuthMsg	1.100.1.4	accessible-for-notify	DisplayString	
rsuSignatureVerifyMsg	1.100.1.5	accessible-for-notify	DisplayString	
rsuAccessMsg	1.100.1.6	accessible-for-notify	DisplayString	
rsuTimeSourceLostMsg	1.100.1.7	accessible-for-notify	DisplayString	
rsuClockSkewMsg	1.100.1.8	accessible-for-notify	DisplayString	
rsuTimeSourceMismatchMsg	1.100.1.9	accessible-for-notify	DisplayString	
rsuGpsAnomalyMsg	1.100.1.10	accessible-for-notify	DisplayString	
rsuGpsDeviationMsg	1.100.1.11	accessible-for-notify	DisplayString	
rsuGpsNmeaNotifyInterval	1.100.1.12	read-write	Integer32	0..18000
rsuAlertLevel	1.100.1.13	accessible-for-notify	INTEGER	0..4

Appendix C. Active Message File Format

The format for both encoded Store & Repeat Messages and encoded Immediate Forward messages is contained below

```
# Message File Format
# Modified Date: 04/10/2014
# Version: 0.7
Version=0.7
#
# Message Dispatch Items
#
# All line beginning with # shall be removed in file sent to radio
#
# Message Type
# Values: SPAT, MAP, TIM, (other message types)
Type=<Type>
#
# Message PSID as a 2 Byte Hex value (e.g. 0x8003)
PSID=<PSID>
#
# Message Priority in the range of 0 (lowest) through 7
Priority=<priority>
#
# Transmission Channel Mode
# Allowed values: CONT, ALT
TxMode=<txmode>

# Allowed values: 172, CCH, SCH (note: “CCH” refers to DSRC Channel 178 and SCH refers to the #operator configured DSRC Service Channel)
TxChannel=<channel>
#
# Transmission Broadcast Interval in Seconds
# Allowed values: 0 for Immediate-Forwarding, 1 to 5 for Store-and-Repeat
TxInterval=<txinterval>
#
# Message Delivery (broadcast) start time (UTC date and time) in the form:
# "mm/dd/yyyy, hh:mm”
# Leave value blank if Immediate Forward mode
DeliveryStart=<mm/dd/yyyy, hh:mm>
#
# Message Delivery (broadcast) stop time (UTC date and time) in the form:
# "mm/dd/yyyy, hh:mm”
# Leave value blank if Immediate Forward mode
DeliveryStop=<mm/dd/yyyy, hh:mm>
#
# Message Signature/Encryption
Signature=<True/False>
Encryption=<True/False>
#
```

# Message Payload (encoded according to J2735 or other definition)
Payload=<DSRC message payload>

Appendix D. Example WAVE Service Advertisement (WSA)

Context

Figure D-1 indicates the context for an example Signed WSA format, as indicated in IEEE 1609.3-2016.

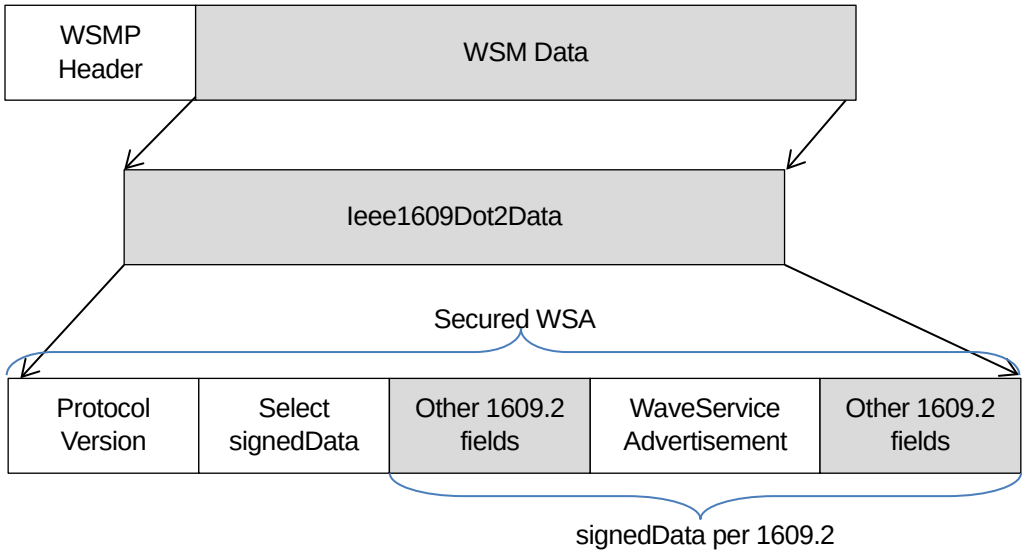

Figure D-1. Diagram. Context for Example WAVE Service Advertisement Format.

WSA Example

Table D-1 provides the format of a basic WSA for an RSU that advertises Intersection Safety Awareness and IPv6 Routing services

Table D-1: Format of a Basic WSA for an RSU.

Header	WSA Version and Option Indicator	0x3F	WSA Version = 3 (4 bits) Option Indicator = 0b1111 (4 bits) (all Header Extensions are present
	WSA ID and Content Count	0x11	WSA ID =1 (4 bits) Content Count = 1 (4 bits)
	Repeat Rate	32	indicates the WSA is repeated 50 times per 5 seconds
	3DLocation		based on RSU Location
	Advertiser ID		ASCII content representing the RSU Owner

Service Info Segment 1	PSID	0x82	Intersection Safety Awareness
	Channel Index	0x09	Chan Index = 1 (5 bits) reserved = 0b00 (2 bits) Opt Ind=0b1 (1 bit)
	PSC	0x49 6E 74 65 72 73 65 63 74 69 6F 6E 20 53 61 66 65 74 79 20 41 77 61 72 65 6E 65 73 73	ASCII representation of "Intersection Safety Awareness"
	RCPI Threshold		-95dBm
	WSA Count Threshold	5	5: Indicates the receiving devices should ignore the Advertised Services if it receives less that 5 WSAs. Note: The WSA Count Threshold Interval is not present, indicating a default value of 1 second
Service Info Segment2	PSID	0x10 20 40 7E	IPv6 Routing
	Channel Index	0x11	Chan Index = 2 (5 bits) reserved = 0b00 (2 bits) Opt Ind=0b1 (1 bit)
	PSC	0x49 50 76 36 20 52 6F 75 74 69 6E 67	ASCII representation of "IPv6 Routing"
	RCPI Threshold		-90dBm
	WSA Count Threshold	5	5: Indicates the receiving devices should ignore the Advertised Services if it receives less that 5 WSAs. Note: The WSA Count Threshold Interval is not present, indication a default value of 1 second

Channel Info Instance Advertise SPaT and Map	Operating Class	0x0E	14
	Channel Number	0xAC	indicates this service is offered on SCH 172
	Transmit Power	0x14	20dBm
	Adaptable and Data Rate	0x0C	Adaptable = Fixed Data Rate = 6 Mbs
	Channel Info Option Indicator	1	indicates the presences of Element Extensions
	Channel Access	0	Continuous Access during both Time Slot 0 and Time Slot 1

Channel Info Instance Advertise IPv6 Routing	Operating Class	0x0E	14
	Channel Number		indicates the SCH in which Service is offered (deployment specific)
	Transmit Power	0x14	20dBm
	Adaptable and Data Rate	0x0C	Adaptable = Fixed Data Rate = 6 Mbs
	Channel Info Option Indicator	0x01	indicates the presences of Element Extensions
	Channel Access	0x02	Alternating Access during Time Slot 1 only
WRA	Router Lifetime		(deployment specific)
	IP Prefix		
	Prefix Length		
	Default Gateway		
	Primary domain name system (DNS)		
	Secondary DNS		
	Gateway MAC Address		

U.S. Department of Transportation
ITS Joint Program Office-HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free “Help Line” 866-367-7487
www.its.dot.gov

FHWA-JPO-17-589

U.S. Department of Transportation