A Project Document of the RSU Standard Working Group

DRAFT

RSU ConOps v01.06

Concept of Operations (ConOps) for the Roadside Unit (RSU) Standard

Draft v01.06 – July 12, 2020

This Concept of Operations is part of the development of an RSU Standard. When the standard is published, it will supersede the USDOT's DSRC Roadside Unit (RSU) Specifications Document v4.1.

Recent Minor Version Revision History

Filename	Date	Author	Notes
RSU_Std_v01_ConOps_v0106_200712	07/02/20	Boaz	Changes made based on adjudication of comments received on ConOps v01.05.
RSU_Std_v01_ConOps_v0105_200605	06/05/20	Boaz	Changes based on decisions made during the ConOps Walkthrough. Document distributed to WG for review and comment.
RSU_Std_v01_ConOps_v0104_200528	05/28/20	Boaz	Name change and typo correction. Version used for ConOps Walkthrough June 1-2, 2020.
RSU_Std_v5_ConOps_v0104_200524	05/24/20	Boaz	Edits post WG Mtng 05/22/20.
RSU_Std_v5_ConOps_v0103_200521	05/21/20	Boaz	Edits post WG Mtng 05/20/20.
RSU_Std_v5_ConOps_200520a	05/20/20	Boaz	Edits during WG Mtng 05/20/20.
RSU_Std_v5_ConOps_200520	05/20/20	Boaz	Complete ConOps including architectural diagrams prior to WG Mtng 05/20/20.
RSU_Std_v5_ConOps_200519_JP_RR	05/20/20	Chan	Combined edits from JP, RR
RSU_Std_v5_ConOps_200519	05/19/20	Boaz	Edits from PXC, WB, JPM, JA, and RB
RSU_Combined ConOps Contributions-200515edits.docx	05/15/20	Chan	Edits from 5/15/20 SME meeting
RSU_Combined ConOps Contributions-200513edits+JPM to JP.docx	05/15/20	Crowe	Additional edits from JPM and JA.
RSU_Combined ConOps Contributions-200513edits.docx	05/13/20	Chan	Edits from 5/13/20 SME meeting
RSU_Combined ConOps Contributions.docx	05/13/20	Crowe	Combined initial contributions

Foreword

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

CONTENTS

Page

FIGURES

Section 1
General Information [Informative]

1.1 Scope

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

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

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

1.2 References

1.2.1 Normative References

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

Identifier	Title
3GPP TS 23.285	Architecture Enhancements for V2X Services, 3GPP.
IEEE 802.3-2018	IEEE Standard for Ethernet, IEEE, 2018.
IEEE 802.11-2016	IEEE Standard for Information technology--Telecommunications and information exchange between systems local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (IEEE802dot11-MIB in Annex A.3).
IEEE 1609.2-2016	IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages, IEEE, 2016.
IEEE 1609.2a-2017	IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages - Amendment 1, IEEE, 2017.
IEEE 1609.3-2020?	IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Networking Services, IEEE 2020.
IEEE 1609.4-2016	IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation, IEEE, 2016.
ISO/TS 21177:2019	Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices.
NIST FIPS 140-3	Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, March 22, 2019.
NTCIP 1218 v01	Object Definitions for Roadside Units (RSUs), AASHTO / ITE / NEMA, published xxxx 2020.
SAE J2735_2020xxxx	V2X Communications Message Set Dictionary™, SAE.
SAE J2945_201712	Dedicated Short Range Communication (DSRC) Systems Engineering Process Guidance for SAE J2945/X Documents and Common Design Concepts.

1.2.2 Other References

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

Identifier	Title
U.S. Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT)	Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT), USDOT.
FHWA-JPO-17-589	DSRC Roadside Unit (RSU) Specifications Document v4.1, USDOT, Saxton Transportation Operations Laboratory, published April 28, 2017. Note: Also referred to as RSU Specifications 4.1.
NEMA TS 10-2019 v20	Connected Vehicle Infrastructure - Roadside Equipment, NEMA, Final first draft, December 19, 2019.
ATC 5201 v06A	Advanced Transportation Controller (ATC) Standard Version 06A," ATC Joint Committee, July 2020.
ATC 5401 v02A	Application Programming Interface (API) Standard for the Advanced Transportation Controller (ATC) Version 02A, ATC Joint Committee, July 2020.
NTCIP 1202 v03A	Object Definitions for Actuated Signal Controllers (ASC) Interface. AASHTO/ITE/NEMA, published May 2019.
FCC Title 47, Part 90	Federal Communications Commission (FCC) Code of Federal Regulations (CFR) Title 47: Telecommunication, Part 90 – Private Land Mobile Radio Services.
ISO/IEC/IEEE 24765:2017	ISO/IEC/IEEE International Standard – Systems and Software Engineering – Vocabulary.

1.2.3 Contact Information

1.2.3.1 Internet Documents

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

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

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

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

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

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

1.2.3.3 FHWA Documents

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

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

1.2.3.4 IEEE Standards

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

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

1.2.3.5 ISO, IEC, and ISO/IEC Standards

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

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

1.2.3.6 NTCIP Standards

Copies of NTCIP standards may be obtained from:

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

1.2.3.7 SAE International Documents

Copies of SAE International documents may be obtained from:

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

1.2.3.8 3GPP Documents

Copies of 3GPP documents may be obtained electronically from:

http://www.3gpp.org/

1.3 Terms

The following terms, definitions, acronyms, and abbreviations are used in this document. Electrical and electronic terms not defined here are used in accordance with their definitions in IEEE 100-2000. English words not defined here or in IEEE 100-2000 are used in accordance with their definitions in Webster's New Collegiate Dictionary.

Term	Definition
Coordinated Universal Time (UTC)	UTC is the time standard commonly used across the world. The world's timing centers have agreed to keep their time scales closely synchronized – or coordinated. This 24-hour time standard is kept using highly precise atomic clocks combined with the Earth's rotation. UTC is similar to Greenwich Mean Time, but while UTC is a time standard, GMT refers to a time zone (similar to Eastern Standard Time). UTC never changes to account for daylight savings time. Note: UTC may have different references. RSU Specifications 4.1 is based on 1/1/1970 while IEEE 1609.2 security is based on 1/1/2004 and needs to adjust for leap-year seconds.
Dedicated Short Range Communications (DSRC)	A V2X communications interface conforming to IEEE 802.11.
Interchangeability	A condition which exists when two or more items possess such functional and physical characteristics as to be equivalent in performance and durability, and are capable of being exchanged one for the other without alteration of the items themselves, or adjoining items, except for adjustment, and without selection for fit and performance. (National Telecommunications and Information Administration, U.S. Department of Commerce).
Interoperability	The ability of two or more systems or components to exchange information and use the information that has been exchanged (ISO/IEC/IEEE 24765-2017 International Standard – Systems and software engineering – Vocabulary).
Mobile Unit (MU)	A device used to wirelessly communicate with other devices for safety and mobility purposes carried by a pedestrian, bicyclist, work zone worker, or other traveler.
On-Board Unit (OBU)	A device used to wirelessly communicate with other devices for safety and mobility purposes installed in a vehicle as original equipment or as aftermarket equipment (sometimes referred to as an "aftermarket safety device (ASD)".
Operator	A user of a traffic management system or back-office system. An operator may be located in a traffic management center, co-located with some other back-office system, or work with a system from a remote location.
Roadside Cabinet Electronics (RSCE)	These are the electronics necessary to physically integrate the V2X technology into an on-street enclosure. Typically, one used for a transportation field cabinet system but other enclosures are not excluded.
Roadside Equipment (RSE)	A broad term that includes the RSU and other ITS field equipment (includes traffic signal controllers).
Roadside Unit (RSU)	A transportation infrastructure communications device located on the roadside that provides V2X connectivity between OBUs/MUs and other parts of the transportation infrastructure including traffic control devices, traffic management systems, and back-office systems. Note: Devices that are not part of the transportation infrastructure, such as cellular base stations or satellites, are not RSUs.

Term	Definition
Security Credential Management System (SCMS)	A system of certificate authorities and supporting 6 entities to support distribution of trust in a system based on IEEE 1609.2 digital certificates.
Traffic Signal Controller (TSC)	A field hardened computing device that runs the application program(s) for a transportation field cabinet system. Historically, TSCs run a single application program. TSCs that conform to the ATC 5201 and ATC 5401 standards, use modern processors, a Linux operating system, and can run multiple application programs concurrently on a single controller unit.
Transportation Field Cabinet System (TFCS)	The on-street system used to perform various transportation applications. The most common applications are traffic signal control, ramp metering, and data collection.
Traveler	A motorist, pedestrian, cyclist, or other multimodal user of the transportation infrastructure.
Vulnerable Road User (VRU)	A term applied to those most at risk in traffic, i.e. those unprotected by an outside shield. VRUs are pedestrians (especially children, seniors and people with disabilities), bicyclists, and motor cyclists.
V2X Interface	A logical component of the RSU representing the wireless interface between the RSU and OBUs/MUs.

1.4 Abbreviations

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

3GPP	3rd Generation Partnership Project
AASHTO	American Association of State Highway Transportation Officials
API	Application Programming Interface
ARC-IT	Architecture Reference for Cooperative and Intelligent Transportation
ASC	Actuated Signal Control
ATC	Advanced Transportation Controller
BSM	Basic Safety Message
C-ITS	Cooperative Intelligent Transportation Systems
CA	Certificate Authority
CFR	Code of Federal Regulations
ConOps	Concept of Operations
CORS	Continuously Operating Reference Station
CRL	Certificate Revocation List
CV	Connected Vehicle
CVRE	Connected Vehicles Roadside Equipment
CVRIA	Connected Vehicle Reference Implementation Architecture

DSRC	Dedicated Short Range Communications
EMI	Electromagnetic Interference
ESD	Electrostatic Discharge
FCC	Federal Communications Commission
FHWA	Federal Highway Administration
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
FO	Functional Object
GMT	Greenwich Mean Time
GNSS	Global Navigation Satellite System
HSM	Hardware Security Module
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IOO	Infrastructure Owner Operator
IP	Internet Protocol
ISO	International Organization for Standardization
ISO/TS	ISO Technical Specifications
IT	Information Technology
ITE	Institute of Transportation Engineers
ITS	Intelligent Transportation Systems
JPO	USDOT ITS Joint Program Office
LCCF	Local Certificate Chain File
LPF	Local Policy File
MAP	Intersection Geometry Message
MU	Mobile Unit
NEMA	National Electrical Manufacturers Associations
NIST	National Institute of Standards and Technology
NTCIP	National Transportation Communications for ITS Protocol
NTRIP	Network Transport of RTCM via Internet Protocol
OBU	On-Board Unit
OEM	Original Equipment Manufacturers
PoE	Power over Ethernet
RFC	Request for Comment
RFI	Radio Frequency Interference

ROSA P	Repository and Open Science Access Portal
RSCE	Roadside Cabinet Electronics
RSE	Roadside Equipment
RSM	Road Safety Message
RSPA	Roadside Processing Application
RSU	Roadside Unit
RSU WI	Roadside Unit Wireless Interfaces
RWM	Road Weather Message
SAE	SAE International (formerly Society of Automotive Engineers)
SCA	Signal Control Application
SCMS	Security Credential Management System
SDO	Standards Development Organizations
SE	Systems Engineering
SNMP	Simple Network Management Protocol
SPaT	Signal Phase and Timing or Signal Phase and Timing Message
TFCS	Transportation Field Cabinet System
TIM	Traveler Information Message
TLS	Transport Layer Security
TMC	Traffic Management Center
TMS	Traffic Management System
TSC	Traffic Signal Controller
TSCBM	Traffic Signal Controller Broadcast Message
US	United States
USDOT	United States Department of Transportation
UTC	Coordinated Universal Time (also called “Common Universal Time”)
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VRU	Vulnerable Road User
WAVE	Wireless Access in Vehicular Environment
WSMP	WAVE Short Message Protocol

Section 2
Concept of Operations [Normative]

2.1 Tutorial [Informative]

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

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

The remaining sections of this ConOps are as follows:

- Section 2.2 – Current Situation and Problem Statement [Informative] – This section describes the current situation and issues that have led to the need for an RSU Standard.
- Section 2.3 Operational Architecture [Informative] – This section describes the operational architectures for RSUs that are known to exist.
- Section 2.4 RSU Architecture [Informative] – This section describes the logical architecture of an RSU.
- Section 2.5 Needs [Normative] – This section identifies the user needs for the RSU.
- Section 2.6 Relationship to the ITS National Architecture [Informative] – This section describes how the RSU fits into the ITS National Architecture.

2.2 Current Situation and Problem Statement [Informative]

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

Figure 1 shows the high-level structure of a V2X system. Roadside units (RSUs) are the key element of the system, since they exchange data with OBUs/MUs and other infrastructure elements. RSUs can receive messages from OBUs/MUs and forward these messages to transportation infrastructure elements (e.g., traffic management systems, traffic signal controllers (TSCs), back-office data storage) to provide information about real-time traffic conditions. Similarly, RSUs broadcast real-time critical infrastructure information, such as Signal Phase and Timing (SPaT), information about the intersection’s geometry

(MAP), and Traveler Information (TIM), over the air to OBUs/MUs to inform travelers of current and upcoming traffic management strategies, conditions, and incidents.

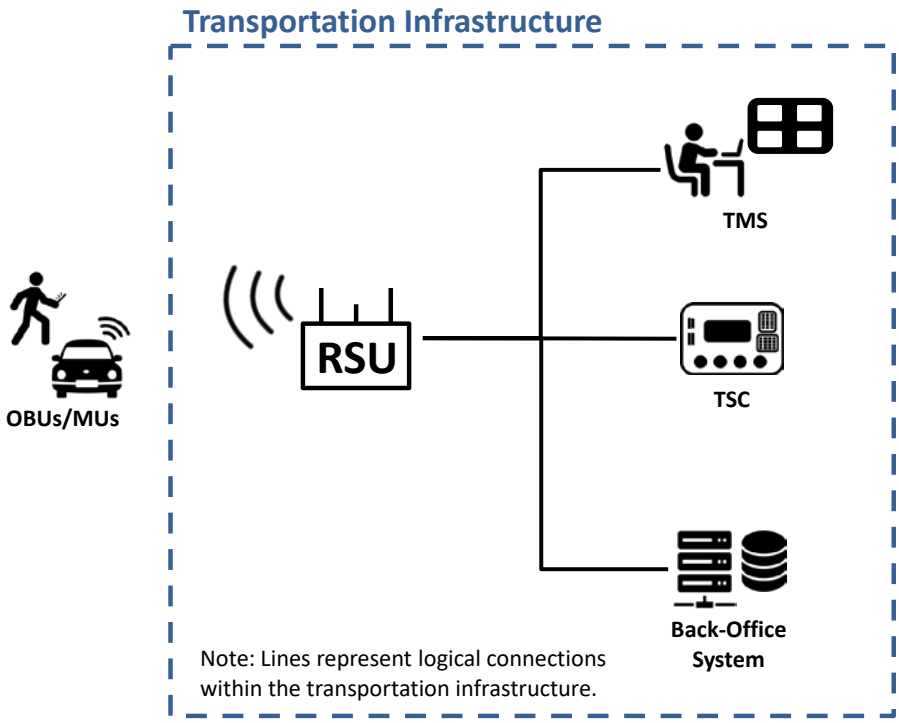

Figure 1 V2X System.

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

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

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

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

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

2.3 Operational and Physical Architecture [Informative]

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

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

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

Roadside Unit (RSU) – Performs the data exchange between OBUs/MUs and infrastructure elements. An RSU may be a single device or the RSU may be distributed between different devices to meet the operational needs of the IOO.

Roadside Unit Wireless Interfaces (RSU WI) – Part of a distributed RSU architecture where the unit mounted on a pole or mast arm only contains the electronics necessary for the radio interfaces of the RSU. The message processing function the RSU is performed in a different device.

Transportation Field Cabinet – Contains the Transportation Field Cabinet System (TFCS) used to perform on-street transportation applications. The most common applications are intersection control, ramp metering, and data collection. The most significant device in a TFCS is the TSC.

Traffic Signal Controller (TSC) – A field hardened computing device that runs the application program(s) for a transportation field cabinet system. Historically, TSCs run a single application program. TSCs that conform to the ATC 5201 and ATC 5401 standards, use modern processors, a Linux operating system, and can run multiple application programs concurrently on a single TSC unit.

Signal Control Application (SCA) – The application program that runs in a TSC to perform the function of operating an intersection.

Roadside Processing Application (RSPA) – The application program that runs in an RSU, TSC or other device to perform the message processing function of an RSU. Unless stated otherwise, the RSPA is a part of the RSU.

Roadside Cabinet Electronics (RSCE) – These are the electronics necessary to physically integrate the RSU into the TFCS.

Traffic Management System (TMS) – The system used by traffic operations staff to configure, control, monitor, and collect data from the TFCS in order to manage traffic.

Back-Office System – Separate system for storage and processing of connected vehicle and device data..

On-Board Unit / Mobile Unit (OBU/MU) – Perform the data exchange between the RSU and non-infrastructure devices. On-Board Units may be installed in motor vehicles (integrated or aftermarket) and MUs may be integrated with cellular phones or otherwise be carried by pedestrians, cyclists, other travelers, or workers in the roadway.

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

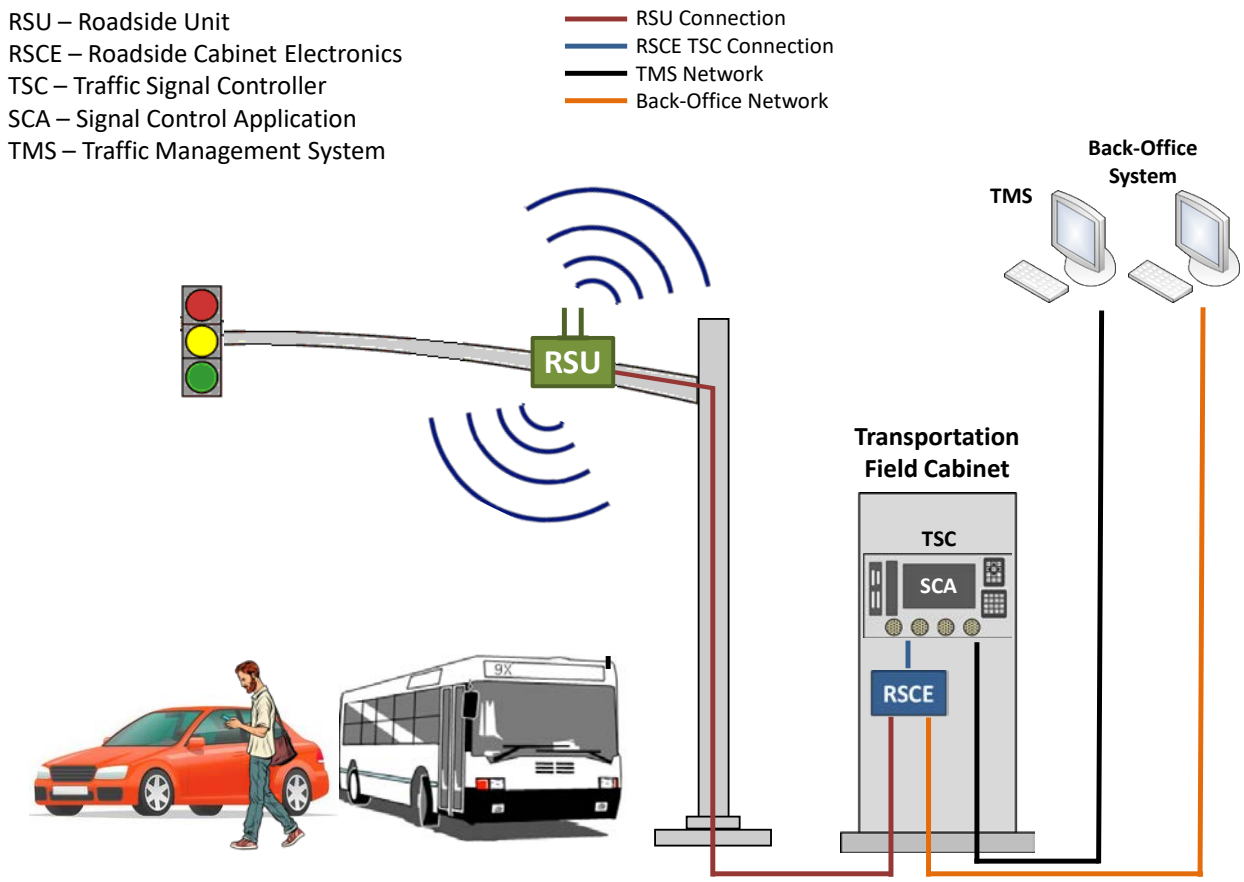

Figure 2 Example of an RSU mounted on a mast arm of a traffic signal.

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

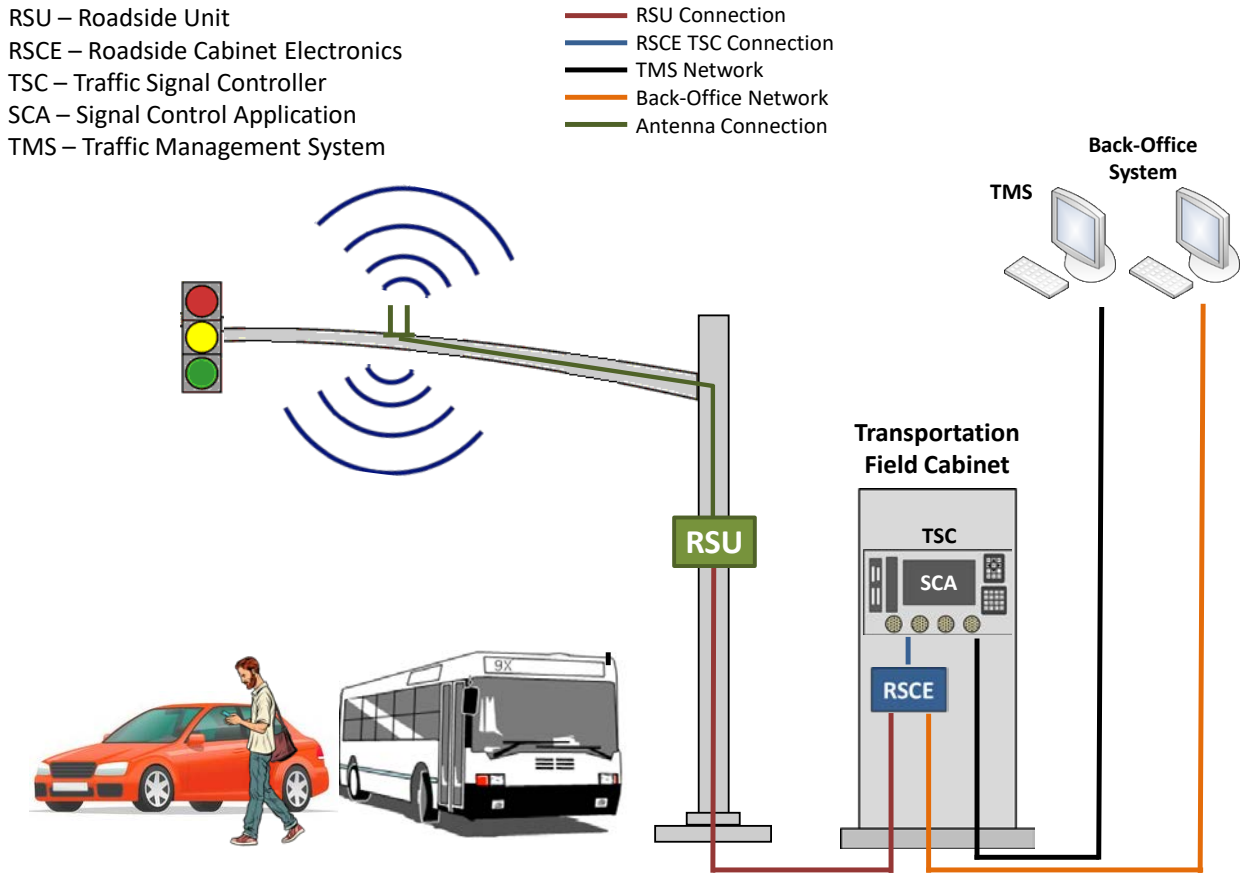

Figure 3 Example of an RSU mounted on a pole with antennas mounted on the mast arm.

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

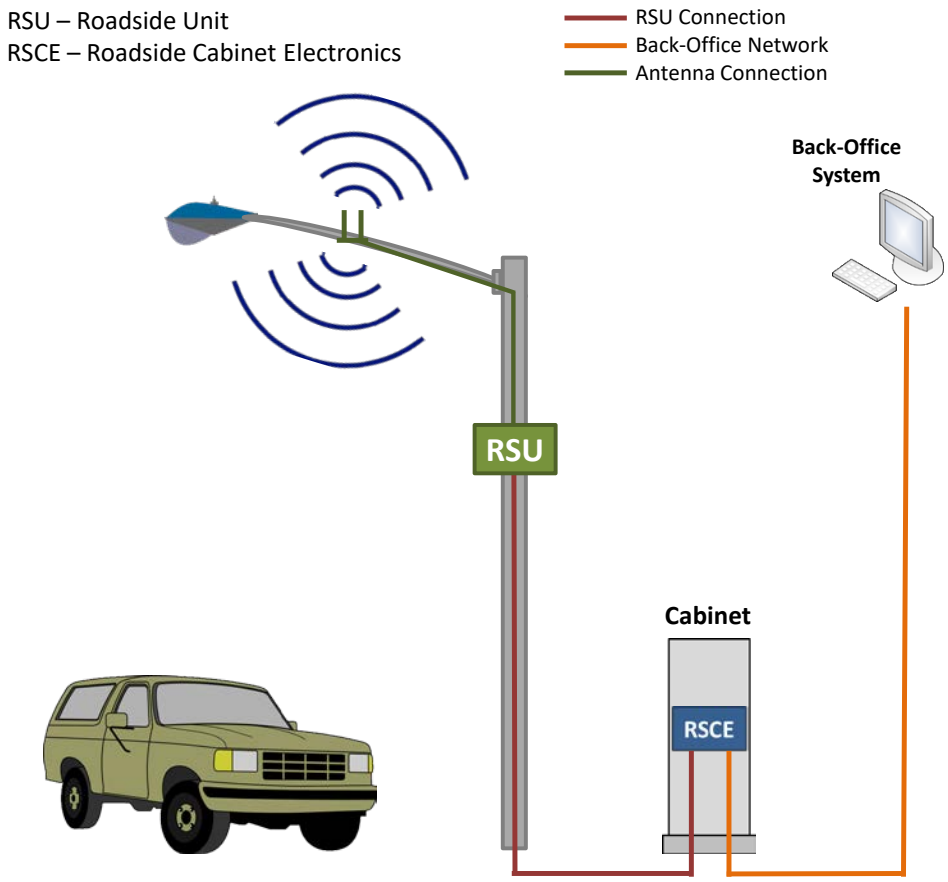

Figure 4 Example of an RSU mounted along a roadway (non-intersection installation).

Figure 5 illustrates an RSU with a distributed functionality. In this case, there is an RSU mounted on a mast arm that contains the V2X and Global Navigation Satellite System (GNSS) antennas and the associated radios. The RSPA is not located in the RSU. The RSU is referred to as the RSU WI to differentiate it from other RSU configurations. In this case, the RSPA is located in the TSC. Typically, the RSU WI connects to the RSCE using Ethernet. Other interfaces may also be supported. The RSCE connects to the TSC using a wired connection (e.g., Ethernet).

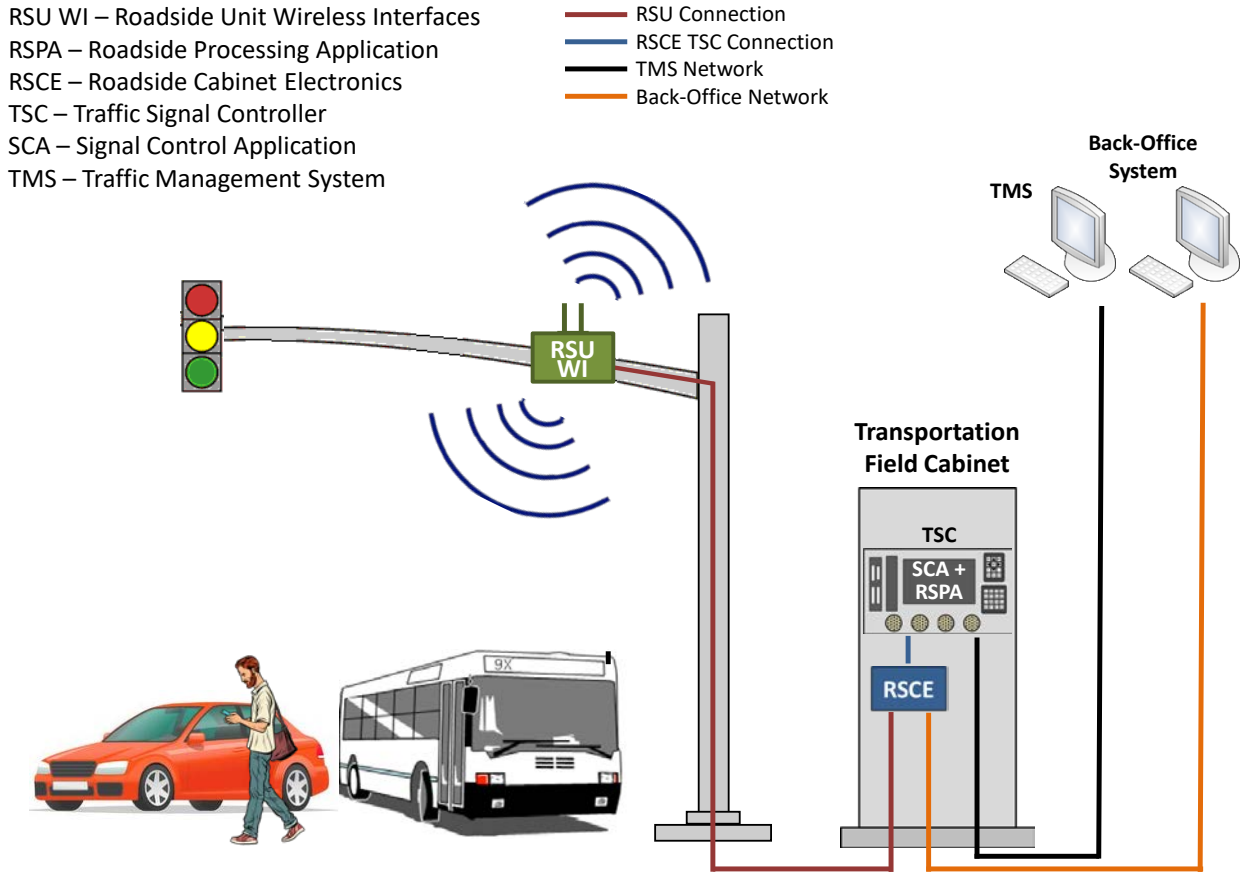

Figure 5 Example of a distributed RSU with the wireless interfaces on the mast arm and the RSU processing application running in a TSC.

2.4 RSU Logical Architecture [Informative]

Figures 6-8 show the logical architectures of an RSU with its elements and connections that correspond to the operational and physical architectures found in the Section 2.3. In addition to the elements listed in Section 2.3 the elements described below are used in the logical architectures.

On-Board Units / Mobile Units (OBUs/MUs) – Devices used to wirelessly communicate with other devices for safety and mobility purposes.

GNSS Satellite – Transmits positioning and timing data to GNSS receivers.

V2X Radio and Antenna – Transmits and receives wireless messages with the OBUs/MUs.

GNSS Receiver and Antenna – Used to receive GNSS positioning information and time.

Figure 6 illustrates the logical connections for the operational architecture and physical layout shown in Figure 2. In this configuration, the RSU contains the RSU processing application and the wireless interfaces including the antennas.

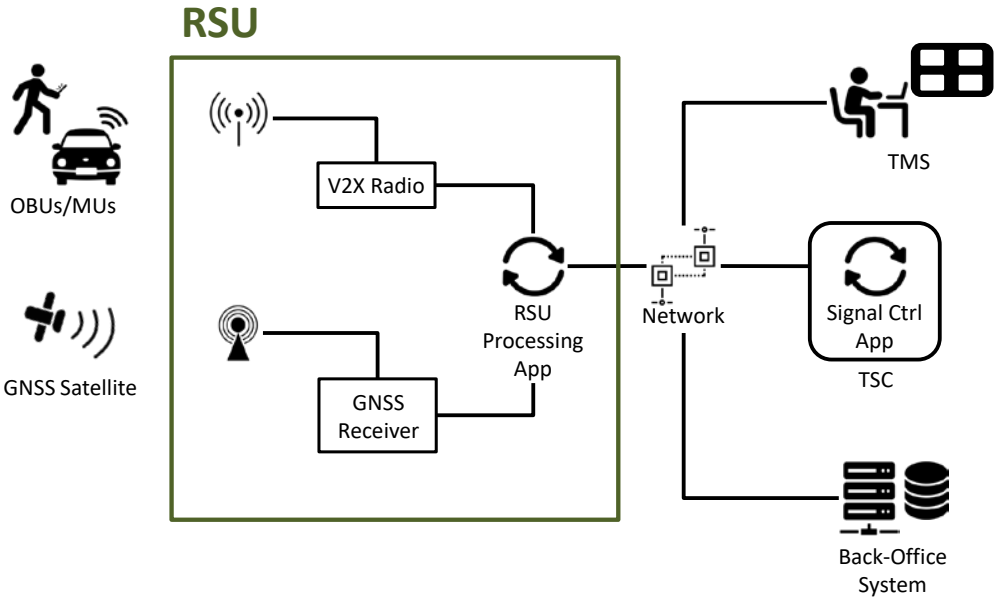

Figure 6 Logical architecture showing an RSU with all of its elements in a single unit.

Figure 7 illustrates the logical architecture for the operational architecture and physical layout shown in Figure 3 and Figure 4. In this configuration, the antennas are mounted separately from the unit.

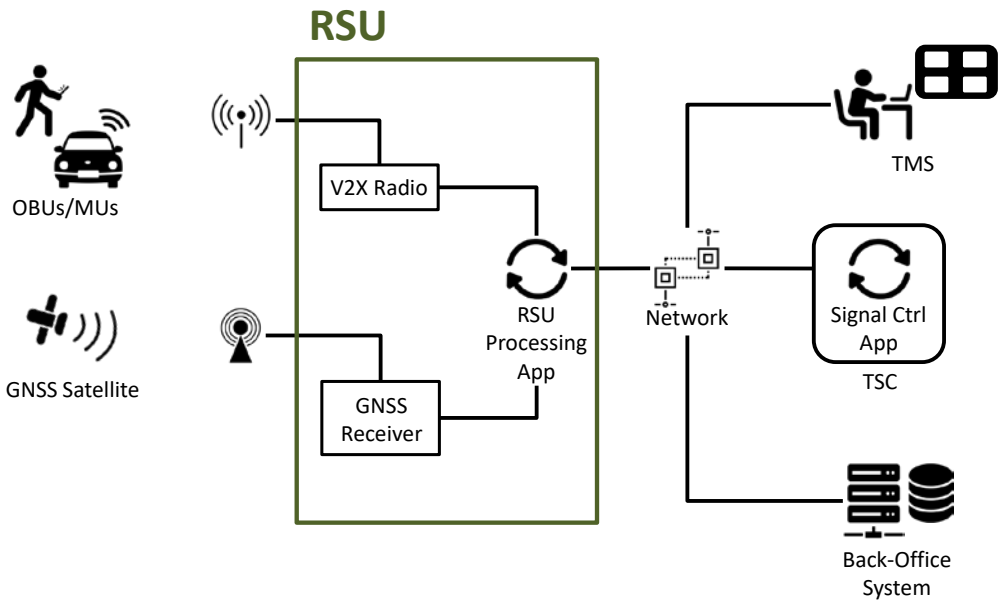

Figure 7 Logical architecture showing an RSU with antennas mounted separately from the unit.

Figure 8 illustrates the logical architecture for the operational architecture and physical layout shown in Figure 5. This represents a distributed configuration of an RSU where the RSU processing application is running in a TSC. The term RSU WI is used to differentiate a unit that only contains the wireless interfaces of the RSU.

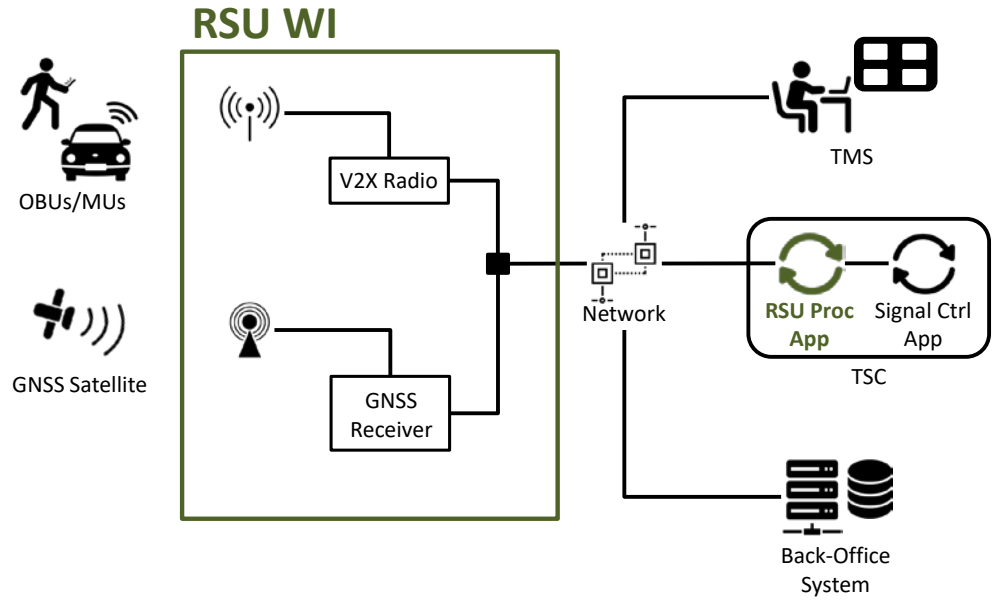

Figure 8 Logical architecture showing a distributed RSU with the RSPA running in a TSC.

2.5 Needs

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

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

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

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

- General, hardware, and mounting needs that concern the overall RSU device;
- Functional needs that concern the primary operational functions of an RSU;
- Behavioral needs that concern the configuration, management, and monitoring of an RSU;
- Local and back-office interface needs that concern the interoperability with OBUs/MUs, transportation field devices, and back-office systems;
- Security needs that concern V2X interface security, local, and back-office interface security, data integrity, certificate management security, and physical security; and
- Certification needs that concern common testing for RSUs.

2.5.1 General/Hardware/Mounting

This section identifies needs that concern the overall RSU device.

2.5.1.1 Operating Voltage

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

2.5.1.2 Extreme Environmental Conditions

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

2.5.1.3 Power Protection and Filtering

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

2.5.1.4 Withstand Vibration and Shock

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

2.5.1.5 Resistant to Electronic Emissions

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

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

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

2.5.1.7 Resistant to Electrostatic Discharge

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

2.5.1.8 Limit Electronic Emissions

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

2.5.1.9 Mounting

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

2.5.1.10 Diagnostic Testing

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

[DEVELOPER NOTE: Jay Parikh to provide requirements in Section 3 to address message accuracy (including SPaT).]

2.5.1.11 Minimize Time for Maintenance Personnel

The RSU needs to be designed to reduce the time required for maintenance personnel to perform maintenance actions in the field. When an RSU is being repaired there can be a safety hazard for both the motorist and the field maintenance personnel. The RSU is to be designed for quick diagnostics, software updates, antenna swap out, and unit switch out.

2.5.1.12 Quality Construction

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

2.5.1.13 Interchangeable

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

2.5.1.14 Software and Firmware Updates

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

2.5.1.15 Size and Weight

The RSU needs to be compact in size and lightweight. RSUs may be installed on signal poles and mast arms where the effects of wind and the weight could hinder deployment.

2.5.1.16 User Safety

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

2.5.2 Functional

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

2.5.2.1 Startup

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

2.5.2.2 Recovery

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

2.5.2.3 Time Keeping

This section identifies needs regarding time keeping on an RSU.

2.5.2.3.1 Track Time

The RSU needs to accurately maintain time. This feature is critical for RSU management and security.

2.5.2.3.2 Time Source

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

2.5.2.4 Determine Current Location

The RSU needs to estimate its current location. This feature allows the RSU and its management system to determine the RSU's location. This facilitates applications that rely on location specific information and monitoring of the RSU's movement. Cryptographic security processes also use location information.

2.5.2.5 Network Interface

The RSU needs to include a network interface. This is used to connect to local field devices and back-office systems and is configured using objects defined in NTCIP 1218 v01.

2.5.2.6 Performance and Monitoring Data

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

2.5.2.6.1 Non-Volatile Operational Logging

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

2.5.2.7 RSU Clustering

The RSU needs to be capable of operating within a set of grouped RSUs. This enables a single application or set of applications to function when the RF coverage environment is challenging. This increases the RF coverage and the number of channels available for use by applications.

2.5.2.8 Message Handling

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

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

2.5.2.8.1 Messages Sent by the RSU

This section identifies needs regarding messages sent by an RSU. It is assumed the messages are already properly encoded. (Note: Revisit this in requirements development).

2.5.2.8.1.1 Immediate forwarding of messages not signed by the message source

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

2.5.2.8.1.2 Immediate forwarding of messages signed by the message source

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

2.5.2.8.1.3 Storing and repeating of messages not signed by the message source

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

2.5.2.8.1.4 Storing and repeating of messages signed by the message source

The RSU needs to forward messages received from local field devices and the back office to the V2X interface. In this case the stored message is already signed and may be encrypted, and the RSU periodically transmits it on the V2X interface. This allows the RSU to periodically send a pre-signed message to OBUs/MUs on behalf of the message source.

2.5.2.8.2 Forwarding of Messages Received by the RSU

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

2.5.2.9 Applications

This section identifies needs regarding the applications of an RSU.

2.5.2.9.1 SPaT Processing

For a signalized intersection, the RSU needs to broadcast Signal Phase and Timing (SPaT) information in real time. This includes communicating with the TSC to receive SPaT information and converting it to SAE J2735 format. It is intended that the RSU support both the NTCIP 1202 v03A SPaT message and the Traffic Signal Controller Broadcast Message (TSCBM) sent from the TSC. This allows the RSU to provide SPaT to the OBUs/MUs.

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

2.5.2.9.2 MAP Messages

The RSU needs to store MAP messages for periodic broadcast over the V2X interface. This enables the OBU/MU to accurately use SPaT information.

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

2.5.2.9.3 Traveler Information Messages

The RSU needs to store TIMs for periodic broadcast over the V2X interface. This feature applies to the J2735 Traveler Information Message (TIM) as well as the Road Weather Message (RWM) and Road Safety Message (RSM) currently in development by SAE. This enables the RSU to provide traveler information to OBUs/MUs.

2.5.2.9.4 BSM Processing

This section identifies needs that concern Basic Safety Message (BSM) processing.

2.5.2.9.4.1 BSM Pre-Processing

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

2.5.2.9.4.2 Wrong Way Driver

The RSU also processes BSMs to detect a wrong way driver. This allows the TMS and IOOs to take action in the event of a wrong way driver.

2.5.3 Behavioral

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

2.5.3.1 Configuration and Management

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

2.5.3.2 Health and Status Monitoring

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

2.5.3.3 Visual Indications

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

2.5.4 Back-Office and V2X Interfaces

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

2.5.4.1 Back-Office Interface

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

2.5.4.2 V2X Interfaces

This section identifies needs regarding V2X interfaces.

2.5.4.2.1 Lower Layers

This section identifies needs for lower layer interfaces on an RSU.

2.5.4.2.1.1 Radio Interfaces

The RSU needs to implement at least one of the following lower layer interfaces:

a) IEEE 802.11 (operating outside the context of a BSS (Basic Service Set) - note: this was originally defined in the 802.11p amendment)
b) 3GPP PC5 mode 4

Note that both technologies may be supported simultaneously. Other technologies may be developed in the future. This allows the RSU to exchange data with OBUs/MUs and facilitates V2X interoperability.

2.5.4.2.1.2 Multi-Channel Operation

The RSU needs to support operation on multiple channels simultaneously. Typically, this implies the availability of at least two lower-layer radios that both implement the same radio interface protocol (both implement IEEE 802.11 or PC5 mode 4). This allows the RSU to exchange data with OBUs/MUs on multiple channels.

Note that there are various options for multi-channel operation described in IEEE 1609.4. The details of what is supported are in Section <section reference in requirements>.

2.5.4.2.2 Network and Transport Layers

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

2.5.5 Security

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

2.5.5.1 Authentication

The RSU needs to authenticate the data exchanged with the OBU/MU. This feature indicates to the OBU/MU that the data transmitted from the RSU is from a "trusted" source. This feature also indicates to the IOO that the data received from the OBU/MU is from a "trusted" source and can be used confidently to manage the roadways.

2.5.5.2 Local and Back Office Interface Security

The RSU needs a secure interface for connection to local field devices and the back office. This interface supports reliable communication with field devices and the software systems in the traffic management

system or back office. This protects the transfer of data between the RSU and connections to the RSU's network interface.

2.5.5.3 Data Integrity

The RSU needs to protect data integrity in accordance with NTCIP 1218 v01. This ensures that the data an RSU transmits is the same as the data the RSU receives from a local field device or back-office system and that it is not corrupted or used for misbehavior.

2.5.5.4 Availability

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

2.5.5.5 Data Confidentiality

The RSU needs to protect the data exchanged with external devices from unauthorized access in accordance with NTCIP 1218 v01. This protects the data when in transit to and from the RSU from being used by hostile parties to attack other local field devices or the back office.

2.5.5.6 Tamper Evident

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

2.5.5.7 Physical Requirement for Certificate Storage

The RSU needs to provide physical protection for access to sensitive information (e.g., private keys) stored on its security module. Having adequate security protections for cryptographic material is a prerequisite for enrollment of the RSU in the Security Credential Management System (SCMS).

Notes:

a) It is important to differentiate that this need aims to protect cryptographic information stored inside the RSU's hardware security module (HSM) from a malicious actor gaining access. The same level of security may not be needed for protecting physical access to the RSU hardware in general.
b) Cryptographic keys used for signing V2X messages may need a higher level of protection up to the point of destroying the keys when tampering with the HSM itself is detected. Lower levels of security, e.g., encrypted file system and tamper evident seals, for preventing access to other information stored on the RSU, e.g., messages being sent, may be sufficient.
c) Information which is usually broadcast via the V2X interface in readable form (e.g., MAP or TIM messages) is not considered sensitive information. Those messages are only signed by the RSU in order to protect data integrity and ensure the origin is a trusted source.

2.5.5.8 Secure Credential Management System

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

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

2.5.5.8.1 SCMS Enrollment

The RSU needs the capability to enroll with an SCMS provider within a secure environment. RSUs enroll (and re-enroll) with an SCMS provider to request application certificates that they can use to sign messages. Note: Enrollment occurs in a secure environment.

2.5.5.8.2 SCMS Connectivity

The RSU needs to connect to an SCMS to request and download new application certificates. This feature allows the RSU to sign messages and allows the IOO to configure what messages the RSU requests certificates for and when the RSU will request new certificates.

2.5.5.8.3 Store Certificates

The RSU needs to securely store the enrollment certificates it uses to interact with the SCMS as well as the application certificates it receives from the SCMS. This feature prevents unauthorized access and use of private keys and certificates.

2.5.5.8.4 Download CRL

The RSU needs to download the Certificate Revocation List (CRL) from the SCMS so the RSU can authenticate signed messages from other devices. Without the CRL, the RSU is not able to authenticate the validity of other devices signatures.

2.5.5.8.5 Download SCMS Files

The RSU needs to download other files associated with the SCMS and certificate operations such as the local policy file (LPF) and local certificate chain file (LCCF). The LCCF is used by devices to determine what certificate authorities (CAs) are in the chain of trust. The local policy file can be used to change some configurations (such as application certificate validity periods) for different locations or regions. This feature allows for deployment-specific certificate configurations and trust between certificate authorities.

2.5.5.8.6 Detect Misbehavior

The RSU needs to detect misbehavior via V2X communications within its wireless coverage area. This feature allows the IOO to determine if an entity or malfunctioning device is causing malicious behavior using V2X communications.

2.5.5.8.7 Report Misbehavior

The RSU needs to report detected misbehavior to the SCMS that it is enrolled with. This feature allows misbehaving devices to be put on a CRL (if verified by the SCMS) and to protect other OBUs/MUs.

2.5.6 Verify Conformance

The RSU needs to be verified for conformance to this standard. This ensures interoperability and compatibility so that safety of life applications can be reliably implemented.

Note – RSUs are typically certified through an industry accepted test procedure. This also includes certification of operation of the RSU in conjunction with standard TSC interfaces.

2.6 Relationship to the ITS National Architecture [Informative]

This section describes which portions of the Architecture Reference for Cooperative and Intelligent Transportation, known as ARC-IT are addressed by the standard. Figure 6 shows the key interfaces from ARC-IT for an RSU (referred to as Connected Vehicle Roadside Equipment in ARC-IT). The diagram

shows the key classes of Physical Objects from the Physical View of ARC-IT: Field, Center, Vehicle, and Personal. A Physical Object is a system or device that provides ITS functionality as part of ITS.

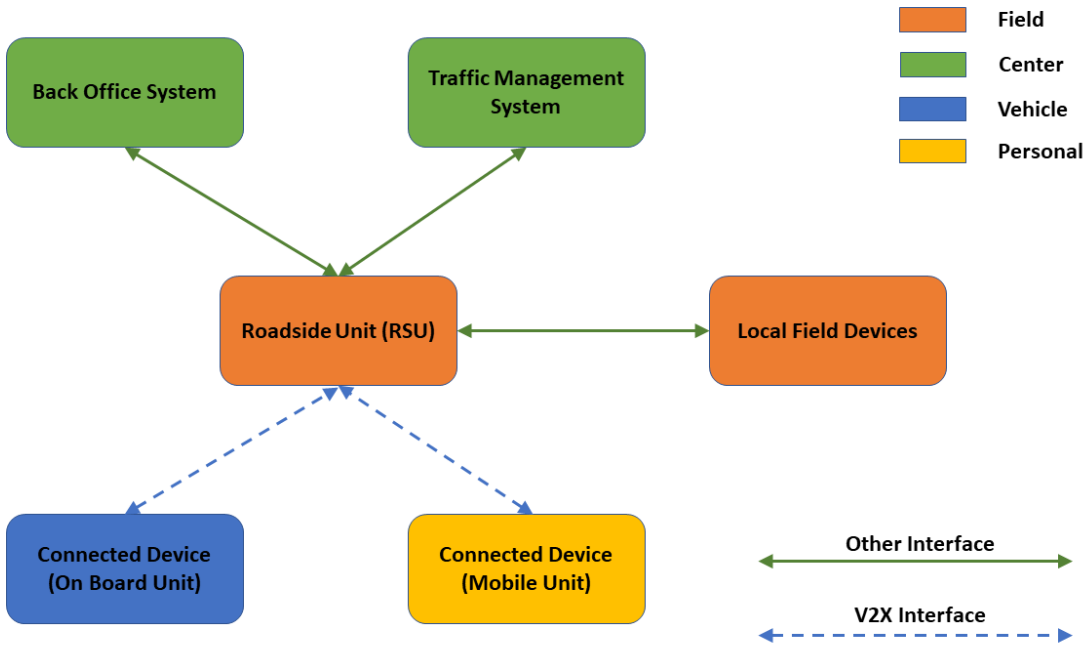

Figure 9 ARC-IT Physical View

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

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

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

- **RSE Device Management.** This FO provides executive control and monitoring of the RSE hardware and installed software applications. It monitors the operational status of the hardware and other attached field devices and detects and reports fault conditions. A back-office interface supports application installation, upgrade, and configuration as well as remote control of the operating mode and hardware configuration settings and initiation of remote diagnostics. A local interface is provided to field personnel for local monitoring and diagnostics, supporting field maintenance, repair, and replacement.

- **RSE Intersection Management.** This FO uses short range communications to support connected vehicle applications that manage signalized intersections. It communicates with approaching vehicles and ITS infrastructure (e.g., the TSC) to enhance traffic signal operations.

Coordination with the ITS infrastructure also supports conflict monitoring to ensure the RSE output and traffic signal control output are consistent and degrade in a fail safe manner.

- **RSE Support Services.** This FO provides foundational functions that support data collection, management, location reference, timing, and data distribution. It coordinates with Support subsystems to maintain necessary registrations with respect to location and scope. It maintains precise location and time information to support other services.

Annex A [Informative]

Position Correction Messages

Position correction messages are useful for mobile-device applications that require precise position (e.g. lane-level accuracy). The immediate forward interface on the RSU (see Sections 2.5.2.8.1.1 and 2.5.2.8.1.2) can be used to send Radio Technical Commission for Maritime Services (RTCM) messages that are already formatted in conformance with SAE J2735. RSU providers may choose to incorporate RTCM-related functionality natively on their RSU. This document does not require native RTCM functionality on the RSU, and this section is included for guidance purposes only.

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

Secure Sessions

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

§