

CTI 4501 v02-ConOps

Connected Transportation Interoperability (CTI)

Connected Intersections Implementation Guide – Final ConOps

Guidance to Setting Up and Operating a Connected
Intersection (CI)

November 20 2023

This document is produced by the Connected Intersections Technical Committee (CTIC).

Published by the following organizations:



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



U.S. Department
of Transportation

The Connected Transportation Interoperability (CTI) family of standards are a series of documents that are jointly developed by stakeholders across the connected vehicle spectrum, including infrastructure owner operators (IOOs), the automotive industries, device manufacturers, mobility data providers, and systems integrators. These stakeholders and many others are represented by the following Standards Development Organizations (SDOs), including American Association of State Highway and Transportation Officials (AASHTO), Institute of Transportation Engineers (ITE), National Electrical Manufacturers Association (NEMA) and SAE International. Sponsored by the United States Department of Transportation (USDOT), documents in the CTI family may be approved and published by any of SDOs mentioned, but are developed and maintained by representatives across the connected vehicle spectrum. The documents in the CTI family includes standards and technical reports that provide guidance to develop and maintain an interoperable connected vehicle environment.

Foreword

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

This CI Implementation Guide addresses the ambiguities and gaps identified by early deployers and provides guidance to generate messages and develop applications for signalized intersections that are interoperable across the United States, especially for the automated transportation systems. This document focuses on harmonizing the existing signal phase and timing (SPaT) messages deployed, using the USDOT sponsored *Cooperative Automated Transportation Clarifications for Consistent Implementations (CCIs) To Ensure National Interoperability Connected Signalized Intersections* as a starting point.

This CI Implementation Guide was developed following a systems engineering process and includes a Needs to Requirements Traceability Matrix (NRTM) and a Requirements Traceability Matrix (RTM). Users of this CI Implementation Guide should use the NRTM and RTM to determine how to design a connected intersection that satisfies their specific needs.

More information on this effort can be found on the [ITE Website](#).

Document History

The following is a summary of the changes to CTI 4501 v02 from CTI 4501 v1.01.

- a) Updated headers, footer, front matter, and reference versions
- b) Updated Section 1, General Information
- c) Updated Section 2, Concept of Operations
- d) Added the following user needs:
 - a. 2.4.2.4 Receive Approaching Vehicle Information from an RSU
 - b. 2.4.4.1.10 Secure Backend

- c. 2.4.4.1.11 Physical Security
- d. 2.4.4.1.12 Device/System Monitoring
- e. 2.4.5 Operations and Maintenance Needs
 - f. 2.4.5.1 Interoperability
 - g. 2.4.5.2 Lifecycle
 - h. 2.4.5.3 Maintenance
 - i. 2.4.5.4 System Diagnostic Interface
 - j. 2.4.5.5 System Performance Monitoring
 - k. 2.4.5.6 System Upgradeability
 - l. 2.8.1.4.3 Verify Performance Needs
- e) Added Annex I, RLVW Deployment - Practioner Approach

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

SAE International

400 Commonwealth Drive
Warrendale, PA 15096

Jennifer Collins, jennifer.collins@sae.org

Jeff Rouce, Jeff.Rouce@sae.org

Justin Sikorski, Justin.Sikorski@sae.org

ITE

1627 Eye Street, NW, Suite 550
Washington, DC 20006

Ashraf Ahmed, aahmed@ite.org

Siva Narla, snarla@ite.org

Tatiana Richey, trichey@ite.org

AASHTO

555 12th Street NW, Suite 1000
Washington, DC 20004

Robert T. White, rwhite@ashto.org

NEMA

1300 North 17th Street, Suite 900
Rosslyn, Virginia 22209

Brian Doherty, Brian.Doherty@nema.org

Steve Griffith, steve.griffith@nema.org

IEEE 1609 Working Group

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

Connected Intersections Technical Committte (CTIC)

Roy Goudy (Chair) Blaine Leonard (Vice-Chair) Patrick Chan

CTI Controller To Applications (C2A) Task Force

John Thai (Chair) Kevin Balke (Vice-Chair) Ralph Boaz

CTI Positioning Task Force

Jim Misener (Chair) Jason Liu (Vice-Chair)

CTI Security Task Force

William Whyte (Chair) Amit Kapoor (Vice-Chair) Drew Van Duren

CTI Systems Integration Task Force

Dmitri Khijniak (Chair) Frank Perry (Vice-Chair)

CTI Testing and Validation Task Force

Jay Parikh (Chair) Ray Starr (Vice-Chair) Richard Deering

Copyright Notice

NOTICE

© 2023 by the American Association of State Highway and Transportation Officials (AASHTO), the Institute of Transportation Engineers (ITE), and the National Electrical Manufacturers Association (NEMA), SAE International.

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

AASHTO, ITE, NEMA, SAE INTERNATIONAL AND THEIR SUPPLIERS DO NOT WARRANT THE PERFORMANCE OR RESULTS YOU MAY OBTAIN BY USING THESE MATERIALS. NEMA, AASHTO, ITE AND THEIR SUPPLIERS MAKE NO WARRANTIES, EXPRESSED OR IMPLIED, AS TO NON-INFRINGEMENT OF THIRD-PARTY RIGHTS, MERCHANTABILITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. IN NO EVENT WILL AASHTO, ITE, NEMA, SAE INTERNATIONAL OR THEIR SUPPLIERS BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY CLAIM OR FOR ANY CONSEQUENTIAL, INCIDENTAL, OR SPECIAL DAMAGES, INCLUDING ANY LOST PROFITS OR LOST SAVINGS ARISING FROM YOUR REPRODUCTION OR USE OF THESE MATERIALS, EVEN IF AN AASHTO, ITE, NEMA, OR SAE INTERNATIONAL REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

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

NRTM and RTM Distribution Permission

To the extent that these materials are distributed by AASHTO / ITE / NEMA / SAE in the form of a Needs to Requirements Traceability Matrix ("NRTM"), AASHTO / ITE / NEMA / SAE extend the following permission:

- a) You may make or distribute unlimited copies, including derivative works of the NRTM, provided that each copy you make or distribute contains the citation "Based on CTI 4501 NRTM. Used by permission. Original text © AASHTO / ITE / NEMA / SAE.";
- b) You may only modify the NRTM by adding text to the Additional Specifications columns for project-unique or vendor-unique features; and
- c) If the NRTM excerpt is made from an unapproved draft, add to the citation "NRTM excerpted from a draft document containing preliminary information that is subject to change."

This limited permission does not include reuse in works offered by other standards developing organizations or publishers, and does not include reuse in works-for-hire, compendiums, or electronic storage devices that are not associated with procurement documents, or commercial hardware, or commercial software products intended for field installation. The NRTM is completed to indicate the features that are supported in an implementation. Contact ITE for information on electronic copies of the NRTM.

Content and Liability Disclaimer

The information in this publication was considered technically sound by the consensus of persons engaged in the development and approval of the document at the time it was developed. Consensus does not necessarily mean that there is unanimous agreement among every person participating in the development of this document. AASHTO, ITE, NEMA, and SAE International standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest in the topic covered by this publication. While AASHTO, ITE, NEMA, and SAE International administer the process and establish rules to promote fairness in the development of consensus, they do not write the document and they do not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in their standards and guideline publications. AASHTO, ITE, NEMA, or SAE International disclaim liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, application, or reliance on this document. AASHTO, ITE, NEMA, and SAE International disclaim and make no guaranty or warranty, express or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will fulfill any of your particular purposes or needs. AASHTO, ITE, NEMA, and SAE International do not undertake to guarantee the performance of any individual manufacturer or seller's products or services by virtue of this standard or guide.

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

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

Additional Contributors and Reviewers

In addition to the SDOs, Committee Members, Task Force co-chairs, and SMEs, there were many others that contributed to the development of this standard and their input and assistance was critical to the final product. The following list includes those who volunteered their time to help both the Task Forces and consultants ensure that the resulting guidance met their needs, and contributed to the input and review during the development of this guide:

Xxx

In addition to the many volunteer efforts, recognition is also given to the following federal agency that supported the effort by providing funding:

- The United States Department of Transportation (USDOT)

User Comment Instructions

The term “User Comment” includes any type of written inquiry, comment, question, or proposed revision, from an individual person or organization, about any CI Implementation Guide content. A “Request for Interpretation” is also classified as a User Comment. User Comments are solicited at any time. In preparation of this standards publication, input of users and other interested parties was sought and evaluated. User Comments are generally referred to the Committee responsible for developing and/or maintaining the CI Implementation Guide. The CTI Committee chairperson, or their designee, may contact the submitter for clarification of the User Comment. When the CTI Committee chairperson or designee reports the CTI Committee's consensus opinion related to the User Comment, that opinion is forwarded to the submitter. The CTI Committee chairperson may report that action on the User Comment may be deferred to a future CTI Committee meeting and/or a future revision of the standards publication.

A User Comment should be submitted to this address:

Institute of Transportation Engineers (ITE)
1627 Eye Street, NW, Suite 550
Washington, DC 20006
e-mail: standards@ite.org

A User Comment should be submitted in the following form:

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

Reason:

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

Table of Contents

Section 1	General Information [Informative]	1
1.1	Scope	1
1.2	References.....	1
1.2.1	Normative References	1
1.2.2	Other References.....	2
1.2.3	Contact Information.....	3
1.2.3.1	3GPP	3
1.2.3.2	Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT)	3
1.2.3.3	CAMP Documents.....	3
1.2.3.4	FHWA Documents	4
1.2.3.5	IEEE Standards.....	4
1.2.3.6	Internet Documents.....	4
1.2.3.7	ITE Standards	4
1.2.3.8	NTCIP Standards	4
1.2.3.9	SAE International Documents	4
1.3	Terms	5
1.4	Abbreviations	7
Section 2	Concept of Operations [Normative]	9
2.1	Tutorial [Informative]	9
2.2	Current Situation and Problem Statement [Informative].....	10
2.3	Reference Physical Architecture [Informative].....	13
2.3.1	Connected Intersection Architecture.....	13
2.3.2	TSC Infrastructure Architecture	14
2.4	Needs.....	16
2.4.1	Architectural Needs	16
2.4.2	Traffic Signal Controller Infrastructure Data	16
2.4.2.1	Provide Signal Timing Data to an RSU.....	16
2.4.2.2	Provide Signal Timing Status to an RSU	16
2.4.2.3	RLVW Support	16
2.4.2.4	Receive Approaching Vehicle Information from an RSU	17
2.4.3	Messages.....	17
2.4.3.1	Message Performance Needs.....	17
2.4.3.1.1	Uniform.....	17
2.4.3.1.2	Robustness	17
2.4.3.1.3	Concise Messages.....	17
2.4.3.1.4	Advanced Notification	17
2.4.3.1.5	Timeliness	18
2.4.3.1.6	Quality Assurance.....	18
2.4.3.2	Generic Message Data Needs	18
2.4.3.2.1	Time Source.....	18
2.4.3.2.2	Message Revision.....	18
2.4.3.2.3	Timestamp	18
2.4.3.3	Signal Timing Data Needs	18
2.4.3.3.1	Intersection Identification	18
2.4.3.3.2	Intersection Status	18
2.4.3.3.3	Current Movement State.....	19
2.4.3.3.4	Next Movement State	19
2.4.3.3.5	Time Change Details	19
2.4.3.3.6	Next Allowed Movement Time	19

	2.4.3.3.7	Enabled Lanes	19
	2.4.3.3.8	Signal Timing and Roadway Indications Synchronization	19
2.4.3.4		Roadway Geometry Data Needs	20
	2.4.3.4.1	Intersection Geometry.....	20
	2.4.3.4.2	Lane Attributes.....	20
	2.4.3.4.3	Allowed Maneuvers.....	20
	2.4.3.4.4	Connections Between Lanes	20
	2.4.3.4.5	Approach Speed Limit Information	20
	2.4.3.4.6	Revocable Lanes	20
	2.4.3.4.7	Road Geometry Accuracy.....	21
	2.4.3.4.8	Signal Timing and Roadway Geometry Synchronization	21
2.4.3.5		Positioning Data Needs.....	21
	2.4.3.5.1	Positioning Corrections Data Format.....	21
	2.4.3.5.2	Real-Time Kinematic Corrections	21
2.4.4		Security.....	21
	2.4.4.1	Correct Operations.....	21
	2.4.4.1.1	Operations - Data Trustworthiness	21
	2.4.4.1.2	Data Processing.....	22
	2.4.4.1.3	Input Validation	22
	2.4.4.1.4	Cyber Attacks.....	22
	2.4.4.1.5	Cyber Attacks Recovery	22
	2.4.4.1.6	Resilience	22
	2.4.4.1.7	Secure Administration.....	22
	2.4.4.1.8	Authenticated Secure Update.....	22
	2.4.4.1.9	Assurance of Correct Network.....	22
	2.4.4.1.10	Secure Backend.....	23
	2.4.4.1.11	Physical Security.....	23
	2.4.4.1.12	Device/System Monitoring	23
2.4.4.2		Data Flow: Communications and Interface Security	23
	2.4.4.2.1	Data Flow Trustworthiness	23
	2.4.4.2.2	Data Integrity.....	23
	2.4.4.2.3	Data Confidentiality.....	23
2.4.4.3		Network Monitoring	23
	2.4.4.3.1	Misbehavior Reporting by Network Administrators.....	23
2.4.4.4		Credential Management.....	23
	2.4.4.4.1	Credential Provisioning	23
	2.4.4.4.2	Management of Untrustworthy Devices	24
	2.4.4.4.3	Credentialing System Access	24
2.4.5		Operations and Maintenance Needs	24
	2.4.5.1	Interoperability.....	24
	2.4.5.2	Lifecycle	24
	2.4.5.3	Maintenance.....	24
	2.4.5.4	System Diagnostic Interface	24
	2.4.5.5	System Performance Monitoring.....	25
	2.4.5.6	System Upgradeability	25
2.5		Operational Policies and Constraints.....	25
2.6		Operational Scenarios	25
2.6.1		Red Light Violation Warning (RLVW) Application.....	26
2.6.2		Signal Timing Scenarios	27
	2.6.2.1	Rest in Green	27
	2.6.2.2	Two or More Signals or Intersections with One Controller	27
	2.6.2.3	Texas Diamond Intersections.....	30
	2.6.2.4	Florida T Intersection	31
	2.6.2.5	User Logic - Outside the "Knowledge" of the Controller	33
	2.6.2.6	High-Intensity Activated Crosswalk Beacon (HAWK)	34

2.6.2.7	Dynamic Lane Use	36
2.7	Relationship to the ITS National Architecture [Informative].....	36
2.8	Testing and Conformity Verification Management.....	37
2.8.1	Testing and Conformance	38
2.8.1.1	Conformance Statement	38
2.8.1.2	Conformance Definitions [Informative].....	38
2.8.1.2.1	Conformance	38
2.8.1.2.2	Conformance Testing.....	38
2.8.1.2.3	Interface	38
2.8.1.2.4	Interoperability	38
2.8.1.2.5	Interchangeability.....	38
2.8.1.3	Testing and Conformance Scope Overview [Informative]	38
2.8.1.3.1	Testing and Conformance Scope Diagram.....	38
2.8.1.3.2	Testing and Conformance Scope Matrix	39
2.8.1.3.3	Clarifying Assumptions	40
2.8.1.3.4	Testing and Conformance Objectives: Operational Verification and Conformance	40
2.8.1.4	Infrastructure Testing	41
2.8.1.4.1	Validate Message Data Needs	41
2.8.1.4.2	Reference Integrity Message Data Needs.....	41
2.8.1.4.3	Verify Performance Needs.....	41
2.8.2	Test Methodology	41
2.8.2.1	Test Methodology Concepts [Informative]	41
2.8.2.2	Test Environment	42
2.8.3	Message Level Testing.....	43
2.8.3.1	Positive Testing.....	43
2.8.3.2	Negative Testing	44
2.8.3.3	Boundary Testing	44
2.8.3.4	Packet Capture Analysis-based Testing.....	44
2.8.3.5	Field Environment Analysis.....	44
2.8.4	Test Documentation.....	44
2.8.5	Requirements Verification Methods.....	45
2.8.6	Test Cases.....	45
2.8.7	Test Coverage	45
2.8.8	Test Procedures.....	46
2.8.9	Identify Existing Test Documentation	46
2.8.10	Configuration and Change Management Needs	46
Section 3	Functional Requirements [Normative].....	47
3.1	Tutorial [Informative]	47
3.2	Needs to Requirements Traceability Matrix.....	47
3.2.1	Notation [Informative].....	48
3.2.1.1	Conformance Symbols.....	48
3.2.1.2	Conditional Status Notation.....	48
3.2.1.3	Support Column Symbols	49
3.2.2	Instructions for Completing the NRTM [Informative].....	49
3.2.2.1	Conformance Definition.....	49
3.2.3	NRTM.....	50
3.3	Requirements.....	68
3.3.1	Architectural Requirements	68
3.3.1.1	IEEE Std 802.11-2016 (DSRC).....	68
3.3.1.1.1	User Priority Levels.....	68
3.3.1.2	3GPP PC5 Mode 4 (Release 14 or 15 (C-V2X)).....	68
3.3.1.2.1	ProSe Per Packet Priority (PPPP)	68
3.3.1.2.2	One Shot Transmission	69

3.3.2	TSC Infrastructure to RSU Requirements	69
3.3.2.1	TSC Infrastructure Signal Timing Data Requirements.....	69
3.3.2.1.1	SPaT Information Messages Requirements.....	69
3.3.2.1.2	TSC Infrastructure SPaT Information Message Transmission Rate	69
3.3.2.1.3	TSC Infrastructure SPaT Information Message Transmission Failure Threshold.....	69
3.3.2.1.4	TSC Infrastructure SPaT Information Average Message Update Latency	70
3.3.2.1.5	TSC Infrastructure Processing Latency	70
3.3.2.2	Signal Timing Status Requirements.....	70
3.3.2.2.1	TSC Infrastructure Manual Control Indication.....	70
3.3.2.2.2	TSC Infrastructure Stop Time Indication.....	70
3.3.2.2.3	TSC Infrastructure Cabinet Flash (Exception Flash) Indication.....	70
3.3.2.2.4	TSC Infrastructure Controller Flash (Operational Flash) Indication	70
3.3.2.2.5	TSC Infrastructure Preemption Operation Indication.....	70
3.3.2.2.6	TSC Infrastructure Priority Operation Indication.....	70
3.3.2.2.7	TSC Infrastructure Fixed Time Control Indication.....	71
3.3.2.2.8	TSC Infrastructure Non-Fixed Time Control	71
3.3.2.3	TSC Infrastructure RLVW Requirements.....	71
3.3.2.3.1	TSC Infrastructure Assured Green End Time (AGET)	71
3.3.2.3.2	TSC Infrastructure Assured Green Period (AGP).....	71
3.3.2.3.3	TSC Infrastructure Minimum End Time With AGP	71
3.3.3	Message Requirements.....	71
3.3.3.1	Message Performance Requirements	71
3.3.3.1.1	Uniform Message Requirements	71
3.3.3.1.2	Robustness Requirements.....	73
3.3.3.1.3	Concise Messages Requirements	73
3.3.3.1.4	Advanced Notification Requirements.....	74
3.3.3.1.5	Timeliness Requirements	74
3.3.3.1.6	Quality Assurance Requirements	74
3.3.3.2	Generic Message Requirements.....	75
3.3.3.2.1	Time Accuracy	75
3.3.3.2.2	Message Revision Requirements	75
3.3.3.2.3	Timestamp Requirements.....	76
3.3.3.3	Signal Timing Data Requirements	76
3.3.3.3.1	Intersection Identification Requirements.....	76
3.3.3.3.2	Intersection Status Requirements.....	76
3.3.3.3.3	Current Movement State Requirements	78
3.3.3.3.4	Next Movement State Requirements.....	79
3.3.3.3.5	Time Change Details Requirements.....	80
3.3.3.3.6	Next Allowed Movement Requirements.....	81
3.3.3.3.7	Enabled Lanes Indication.....	81
3.3.3.3.8	SPaT Message - Accuracy	81
3.3.3.4	Roadway Geometry Data Requirements	81
3.3.3.4.1	Intersection Geometry Requirements	81
3.3.3.4.2	Lane Attributes	84
3.3.3.4.3	Lane Maneuvers	85
3.3.3.4.4	Connections Between Lanes	85
3.3.3.4.5	Speed Limit Information Requirements	86
3.3.3.4.6	Revocable Lanes	86
3.3.3.4.7	MAP Message - Accuracy.....	86
3.3.3.4.8	Signal Timing and Roadway Geometry Information Synchronization	86
3.3.3.5	Positioning Messages	87

	3.3.3.5.1	Positioning Corrections	87
	3.3.3.5.2	Real-Time Kinematics Requirements	87
3.3.4		Security Requirements	87
	3.3.4.1	Connected Intersection System Trustworthiness Requirements	87
	3.3.4.1.1	SPaT Information Message Trustworthiness - RSU	87
	3.3.4.1.2	SPaT Information Message Trustworthiness - TSC Infrastructure	88
	3.3.4.1.3	MAP Data Trustworthiness	88
	3.3.4.1.4	RTCM Corrections Data Trustworthiness	88
	3.3.4.2	Connected Intersection System Security Requirements	88
	3.3.4.2.1	Secure Network	88
	3.3.4.2.2	Assurance of Connection to Correct Network	88
	3.3.4.3	Verification of Connected Intersection System Security Requirements	88
	3.3.4.3.1	Security Compliance Assessment	89
	3.3.4.3.2	Point of Certification	89
	3.3.4.4	Certificate Issuing Requirements	89
	3.3.4.4.1	Certificate Issuance	89
	3.3.4.4.2	Certificate Nonissuance	89
	3.3.4.4.3	CI Operation Security Practices	89
	3.3.4.4.4	RSU Security Standards	89
	3.3.4.4.5	TSC Infrastructure Security Standards	89
	3.3.4.5	Security Against Cyber Attack Requirements	90
	3.3.4.5.1	Cyber-Attack Recovery Plan	90
	3.3.4.5.2	Cyber-Attack Robustness	90
	3.3.4.5.3	Network Protection	90
	3.3.4.6	Data Flow: Communications and Interface Security Requirements	90
	3.3.4.6.1	Interface between RSU and TMS	90
	3.3.4.6.2	Interface between RSU and SCMS	91
	3.3.4.6.3	Interface between an RSU and the OBU/MU	91
	3.3.4.6.4	Interface between an RSU and the TSC Infrastructure	91
	3.3.4.6.5	Interface between the TMS and the TSC Infrastructure	92
	3.3.4.6.6	Interface between the MAP Server and the TMS	92
	3.3.4.6.7	Interface between MAP Server and the SCMS	93
	3.3.4.7	Correct Operations Requirements	93
	3.3.4.7.1	Device Protection Requirements	93
	3.3.4.7.2	Secure Administration of RSU	93
	3.3.4.7.3	RSU Device Class Requirement	95
	3.3.4.7.4	TSC Device Class Requirement	95
	3.3.4.7.5	MAP Signer Device Class Requirement	95
	3.3.4.7.6	Authenticated Secure Update Requirements	95
	3.3.4.8	Network Monitoring Requirements	96
	3.3.4.9	Credential Management Requirements	96
	3.3.4.9.1	Credential Provisioning – (D)TLS Requirements	96
	3.3.4.9.2	Management of Untrustworthy Devices - TLS Requirements ...	96
	3.3.4.9.3	Credential System Access - SCMS Requirements	96
3.4		Testing and Conformance Management	97
	3.4.1	Test Documentation	97
	3.4.1.1	Test Documentation Overview [Informative]	97
	3.4.1.2	Test Plan Requirements	97
	3.4.1.2.1	Test Items	98
	3.4.1.2.2	Features to be Tested	98
	3.4.1.2.3	Features not to be Tested	98
	3.4.1.2.4	Test Coverage	98
	3.4.1.2.5	Item Pass/Fail Criteria	98
	3.4.1.2.6	Requirements to Test Case Traceability Matrix	98
	3.4.1.2.7	Organization Requirements	98

	3.4.1.2.8	Roles and Responsibilities.....	99
	3.4.1.2.9	Resources Summary	99
	3.4.1.2.10	Test Schedule	99
	3.4.1.2.11	Document Procedures and History.....	99
3.4.1.3		Test Case Requirements	99
	3.4.1.3.1	Test Case Identifier.....	99
	3.4.1.3.2	Inputs	99
	3.4.1.3.3	Outcomes.....	100
	3.4.1.3.4	Feature Pass/Fail Criteria	100
	3.4.1.3.5	Intercase Dependencies	100
3.4.1.4		Test Procedure Requirements	100
	3.4.1.4.1	Test Procedure Identifier.....	100
	3.4.1.4.2	Test Case References	100
	3.4.1.4.3	Requirements Verification Method(s)	100
	3.4.1.4.4	Procedure Descriptions.....	101
	3.4.1.4.5	Procedure Steps	101
	3.4.1.4.6	Relationship to other Procedures	102
	3.4.1.4.7	Procedure Special Requirements	102
3.4.1.5		Test Log Requirements.....	102
	3.4.1.5.1	Test Log - Descriptions	102
	3.4.1.5.2	Test Log - Activity and Event Entries.....	102
3.4.1.6		Test Anomaly Report Requirements	103
	3.4.1.6.1	Test Anomaly Report Identifier	103
	3.4.1.6.2	Test Anomaly Report - Date Anomaly Discovered.....	103
	3.4.1.6.3	Test Anomaly Report - Context	103
	3.4.1.6.4	Test Anomaly Report - Description of the Anomaly.....	103
	3.4.1.6.5	Test Anomaly Report - Assessment of Urgency.....	103
	3.4.1.6.6	Test Anomaly Report - Description of the Corrective Action ...	104
	3.4.1.6.7	Test Anomaly Report - Conclusions and Recommendations..	104
3.4.1.7		Conformance Summary Report Requirements.....	104
	3.4.1.7.1	Conformance Summary	104
	3.4.1.7.2	Summary of Testing Activities	104
	3.4.1.7.3	Summary of Testing Task Results.....	104
	3.4.1.7.4	Summary of Anomalies and Resolutions.....	104
	3.4.1.7.5	Summary of Pass/Fail Results.....	105
Section 4		System Design Details [Normative]	106
4.1		Tutorial [Informative]	106
4.2		Requirements Traceability Matrix	106
	4.2.1	Notation [Informative].....	107
		4.2.1.1 Functional Requirement Columns.....	107
		4.2.1.2 Design Details	107
		4.2.1.3 Additional Specifications	107
	4.2.2	Instructions for Completing the RTM [Informative].....	107
	4.2.3	Requirements Traceability Matrix (RTM) Table.....	108
4.3		Design Details.....	120
	4.3.1	Architectural Design Details.....	120
		4.3.1.1 IEEE Std 802.11-2016 (DSRC).....	120
		4.3.1.2 3GPP PC5 Mode 4 (Release 14 or 15 (C-V2X)).....	120
	4.3.2	TSC Infrastructure to RSU Design Details	120
		4.3.2.1 TSC Infrastructure Signal Timing Data Design Details.....	120
		4.3.2.1.1 SPaT Information Messages Design Details	120
		4.3.2.1.2 TSC SPaT Information Message Transmission Rate.....	122
		4.3.2.1.3 TSC SPaT Information Message Transmission Rate Tolerance	122
		4.3.2.1.4 TSC SPaT Information Message Update Latency.....	122

	4.3.2.1.5	TSC Infrastructure Processing Latency	122
4.3.2.2		Signal Timing Status Design Details	122
	4.3.2.2.1	TSC Infrastructure Manual Control Indication Design Detail... ..	122
	4.3.2.2.2	TSC Infrastructure Stop Time Indication.....	122
	4.3.2.2.3	TSC Infrastructure Cabinet Flash (Exception Flash) Indication	123
	4.3.2.2.4	TSC Infrastructure Controller Flash (Operational Flash) Indication	124
	4.3.2.2.5	TSC Infrastructure Preemption Operation Indication.....	125
	4.3.2.2.6	TSC Infrastructure Priority Operation Indication.....	126
	4.3.2.2.7	TSC Infrastructure Fixed Time Control Indication.....	126
	4.3.2.2.8	TSC Infrastructure Non-Fixed Time Control	127
4.3.2.3		TSC Infrastructure RLVW Design Details	127
	4.3.2.3.1	TSC Infrastructure Assured Green End Time (AGET) Design	127
	4.3.2.3.2	TSC Infrastructure Assured Green Period (AGP) Design Details	128
	4.3.2.3.3	TSC Infrastructure Minimum End Time with AGP Design Details	130
4.3.3		Message Design Details	131
	4.3.3.1	Message Performance Design Details.....	131
	4.3.3.1.1	Uniform Message Design Details	131
	4.3.3.1.2	Robustness Design Details.....	139
	4.3.3.1.3	Concise Messages Design Details	139
	4.3.3.1.4	Advanced Notification Design Details.....	142
	4.3.3.1.5	Timeliness Design Details.....	142
	4.3.3.1.6	Quality Assurance Design Details	143
	4.3.3.2	Generic Message Design Details.....	143
	4.3.3.2.1	Time Accuracy	143
	4.3.3.2.2	Message Revision Counter Design Details	143
	4.3.3.2.3	Timestamp Design Details.....	144
	4.3.3.3	Signal Timing Data Design Details	145
	4.3.3.3.1	Intersection Identification Design Details.....	145
	4.3.3.3.2	Intersection Status Design Details.....	146
	4.3.3.3.3	Current Movement State Design Details	149
	4.3.3.3.4	Next Movement State Design Details	151
	4.3.3.3.5	Time Change Details Design Details	153
	4.3.3.3.6	Next Green Design Details	155
	4.3.3.3.7	Enabled Lanes Indication.....	157
	4.3.3.3.8	SPaT Message Accuracy.....	157
	4.3.3.4	Roadway Geometry Data Design Details	157
	4.3.3.4.1	Intersection Geometry Design Details	157
	4.3.3.4.2	Lane Attributes.....	173
	4.3.3.4.3	Lane Maneuvers	176
	4.3.3.4.4	Connections Between Lanes	176
	4.3.3.4.5	Speed Limit Information Design Details.....	178
	4.3.3.4.6	Revocable Lanes	180
	4.3.3.4.7	Map Message – Accuracy.....	180
	4.3.3.4.8	Signal Timing and Roadway Geometry Synchronization	180
	4.3.3.5	Positioning Messages	181
	4.3.3.5.1	Positioning Corrections	181
	4.3.3.5.2	Real-Time Kinematics Design Details	182
4.3.4		Security Design Details.....	184
	4.3.4.1	Connected Intersection System Trustworthiness Design Details	184
	4.3.4.1.1	SPaT Information Message Trustworthiness - RSU.....	184
	4.3.4.1.2	SPaT Information Message Trustworthiness - TSC Infrastructure	184

4.3.4.1.3	MAP Data Trustworthiness	185
4.3.4.1.4	RTCM Corrections Data Trustworthiness	185
4.3.4.2	Connected Intersection System Security Design Details.....	185
4.3.4.2.1	Secure Network	185
4.3.4.2.2	Assurance of Connection to Correct Network.....	185
4.3.4.3	Verification of Connected Intersection System Security Design Details....	185
4.3.4.3.1	Security Compliance Assessment	186
4.3.4.3.2	Point of Certification.....	186
4.3.4.4	Certificate Issuing Design Details	186
4.3.4.4.1	Certificate Issuance	186
4.3.4.4.2	Certificate Nonissuance	187
4.3.4.4.3	CI Operation Security Practices.....	187
4.3.4.4.4	RSU Security Standards	187
4.3.4.4.5	TSC Infrastructure Security Standards	187
4.3.4.5	Security Against Cyber Attack Design Details	187
4.3.4.5.1	Cyber-Attack Recovery Plan.....	187
4.3.4.5.2	Cyber-Attack Robustness	187
4.3.4.5.3	Network Protection.....	188
4.3.4.6	Data Flow: Communications and Interface Security Design Details.....	188
4.3.4.6.1	Interface between RSU and TMS	188
4.3.4.6.2	Interface between RSU and SCMS	191
4.3.4.6.3	Interface between an RSU and the OBU/MU	191
4.3.4.6.4	Interface between an RSU and the TSC Infrastructure	191
4.3.4.6.5	Interface between the TMS and the TSC Infrastructure	192
4.3.4.6.6	Interface between the MAP Server and the TMS	192
4.3.4.6.7	Interface between MAP Server and the SCMS	192
4.3.4.7	Correct Operations Design Details	193
4.3.4.7.1	Device Protection Design Details	193
4.3.4.7.2	Secure Administration of RSU	193
4.3.4.7.3	RSU Device Class Design	195
4.3.4.7.4	TSC Device Class Design.....	195
4.3.4.7.5	MAP Signer Device Class Design	195
4.3.4.7.6	Authenticated Secure Update Design Details.....	196
4.3.4.8	Network Monitoring Design	196
4.3.4.9	Credential Management Design Details	196
4.3.4.9.1	Credential Provisioning – (D)TLS Design Details.....	196
4.3.4.9.2	Management of Untrustworthy Devices – (D)TLS Design Details	197
4.3.4.9.3	Credential System Access – SCMS Design Details	197
Section 5	Connected Intersection Testing [Informative].....	199
5.1	Introduction to CI Test Cases	199
5.1.1	CI Testing Scope and Assumptions.....	199
5.1.2	Approach to the CI Test Cases.....	200
5.2	Requirements to Test Case Traceability Matrix (RTCTM).....	200
5.3	CI SPaT Test Cases	206
5.3.1	CI SPaT Test Case	206
5.3.1.1	CI SPaT Test Case Overview	206
5.3.1.2	SPaT Data Capture 1 – Message Structure and Content.....	206
5.3.2	CI MAP Test Cases	207
5.3.2.1	CI MAP Data Capture Stream Tests	207
5.3.2.2	MAP Data Capture 1 – Message Structure and Content.....	207
5.3.3	CI SPaT-MAP Data Consistency Test Case	207
5.3.3.1	SPaT-MAP Data Consistency.....	208
Annex A	209

A.1	Issues & Rationale	209
A.1.1	NTCIP 1202 v03A Traffic Controller SPaT Data Ambiguity.....	209
	A.1.1.1 Vendor Ambiguity	209
	A.1.1.2 SPaT Generation under Special Situations	209
A.1.2	Conflict between Gap-Based traffic control practices and the predictive signalization needs for RLVW applications	210
A.1.3	Determinism and Consistency for TimeChangeDetails within the SPaT Message.....	210
A.2	Proposed Resolution to NTCIP 1202 Traffic Controller SPaT Data Ambiguity	210
A.2.1	Base Assumptions when Generating SPaT	210
	A.2.1.1 Active TOD Control	210
	A.2.1.2 Active Preemption Control	210
	A.2.1.3 Active Demand.....	210
	A.2.1.4 NTCIP 1202 v03A Configuration.....	211
	A.2.1.5 Soft Flashing Operation	211
	A.2.1.6 Hard Flashing Operation	211
	A.2.1.7 Tech Flash.....	211
	A.2.1.8 Stop Time	212
	A.2.1.9 Manual Control.....	212
	A.2.1.10 Output Mapping.....	212
	A.2.1.11 Proprietary Features	212
	A.2.1.12 Externally Coordinated and/or Adaptively Controlled Intersections.....	213
	A.2.1.13 Post-processed SPaT generation	213
A.2.2	Special Traffic Control Situations.....	213
	A.2.2.1 Changes between Permissive and Protected Movements without a Clearance Interval.....	213
	A.2.2.2 Movement into or Revert from Flashing Operation	214
	A.2.2.3 Bike/Transit Movements.....	214
	A.2.2.4 Green Select Operation	214
A.3	Proposed Resolution to Determinism and Consistency for TimeChangeDetails within the SPaT Message	214
A.3.1	startTime TimeMark OPTIONAL.....	215
A.3.2	minEndTime TimeMark.....	215
A.3.3	maxEndTime TimeMark OPTIONAL	216
A.3.4	likelyTime TimeMark OPTIONAL, (along with TimeIntervalConfidence).....	217
A.3.5	nextTime TimeMark OPTIONAL.....	217
A.4	Recommendations	217
A.4.1	Assumptions of elements to be handled externally from this TF	217
A.4.2	Traffic Controller Vendors	218
A.4.3	NEMA TS-2/ATCC	218
A.4.4	NTCIP 1202 WG	218
A.4.5	SAE J2735 WG	218
A.4.6	ITE.....	218
A.4.7	IOOs.....	218
A.5	NTCIP 1202 Objects: SPaT Generation Conformance	219
A.6	TSCBM and SPaT Data.....	221
A.7	Latency and Timing Error Analysis for Connected Intersections.....	226
A.7.1	Latency	226
A.7.2	Timing Error	228
Annex B Assured Green Period Use Cases [Informative]		229

B.1	Background Information.....	229
B.2	Example Use Case 1	230
B.2.1	No Call on Cross-Street.....	230
B.2.2	Call on Cross-Street at t=9	236
B.2.3	Call On Cross-Street at t=6.....	242
Annex C Additional Information - Positioning [Informative]		247
C.1	RTCM Corrections (MSM4 Messages Only) Broadcast Rate Calculations.....	247
Annex D Security Profiles [Normative]		251
D.1	Security Profile for SPaT Messages	251
D.1.1	Summary.....	251
D.1.2	SPaT PDU Field Use and Convention.....	251
D.1.3	Security Specific Permissions [Normative]	252
D.1.4	IEEE Std 1609.2 Security Profile Identification [Normative]	252
D.1.5	Sending.....	253
D.1.6	Receiving	254
D.1.7	Security Management.....	255
D.2	Security Profile for MAP Messages	255
D.2.1	Summary.....	255
D.2.2	MAP PDU Field Use and Convention	256
D.2.3	Security Specific Permissions [Normative]	256
D.2.4	IEEE Std 1609.2 Security Profile Identification (Normative).....	257
D.2.5	Sending.....	257
D.2.6	Receiving	259
D.2.7	Security Management.....	260
D.3	Security Profile for RTCM corrections	260
D.3.1	Summary.....	260
D.3.2	RTCM PDU Field Use and Convention	261
D.3.3	Uncompressed GPS Correction Information	261
D.3.4	Certificate Issuance Guidance.....	261
D.3.5	Security Specific Permissions [Normative]	261
D.3.6	IEEE Std 1609.2 Security Profile Identification.....	262
D.3.7	Sending.....	262
D.3.8	Receiving	263
D.3.9	Security Management.....	264
Annex E Additional Information - Security [Informative].....		266
E.1	Securing Messages From Source to End Recipient (Example)	266
E.2	Certification Process	267
E.3	Attack Tree Examples.....	269
E.3.1	Introduction	269
E.3.2	Attack Tree Building Preliminaries.....	270
E.3.3	Constructing an Attack Tree: RSU Outputs Incorrect SPaT Messages	271
E.3.4	Constructing an Attack Tree: RSU Outputs Incorrect MAP Messages	274
E.3.5	Constructing an attack tree: "RSU outputs incorrect RTCM messages."	276
Annex F Testing Resources [Informative].....		278

F.1	Existing Test Documentation	278
F.2	Example Usage of a Test Tool	278
F.2.1	Description of OBU-Based Test Tool JSON Log.....	279
F.2.2	Description of OBU-Based Test Tool JSON Log.....	279
F.2.3	Description of OBU-Based Test Tool JSON Log.....	281
Annex G User Requests [Informative]		284
G.1	User Requests - Needs.....	284
G.1.1	Mobility Applications	284
G.1.2	Queue Information at an Intersection	284
G.1.3	Indication of Pedestrians or Bicyclists in a Crosswalk.....	284
G.1.4	Confidence Factor and Likely Time	284
G.1.5	Signal Priority and Preemption	285
G.1.6	Advisory Speeds.....	285
G.1.7	Misbehavior Reporting by OBUs	285
G.1.8	Misbehavior Reporting by IOO Field Devices.....	285
G.1.9	Levels of Testing.....	285
G.2	User Requests - Requirements	285
G.2.1	Quality Assurance.....	285
G.2.2	Computed Lane – Scaling	286
G.2.3	No SPaT Available.....	286
G.2.4	TSCBM	286
G.3	User Requests - Design Details.....	286
G.3.1	Failure Flash	286
G.3.2	Operational Logging – TSC Infrastructure.....	287
G.3.3	Connections	287
G.3.4	Test Cases.....	287
G.3.5	Security Models	287
Annex H Recommendations to SDOs [Informative]		288
H.1	SAE Core Technical Committee - SAE J2735.....	288
H.1.1	DE_TimeMark	288
H.1.2	DF_MovementEventList	288
H.1.3	DE_IntersectionStatusObject.....	289
H.1.4	DF_NodeAttributeSetLL.....	289
H.1.5	DE_RoadRegulatorID	289
H.1.6	DF_TimeChangeDetails.....	289
H.1.7	MAP Message.....	290
H.1.8	Backwards Compatibility.....	290
H.2	NTCIP Actuated Signal Controllers (ASC) Working Group	290
H.2.1	Protected / Permissive Movements	290
H.2.2	Hard Flashing Operation.....	290
H.2.3	Dynamic AWEG Decisions	290
H.2.4	Output Mapping	290
H.2.5	Additional SPaT Elements.....	291
H.2.6	SPaT Data Tables.....	291

H.3	NEMA TS2 Working Group.....	291
H.4	ATC Joint Committee/ITS Cabinet Working Group	291
Annex I RLVW Deployment - Practitioner Approach [Informative].....		292
I.1	Introduction	292
I.1.1	Expectations for the RLVW System Performance.....	292
	I.1.1.1 Delivers Expected Performance and Accuracy.....	292
	I.1.1.2 RLVW is Interoperable	293
	I.1.1.3 Secure	293
	I.1.1.4 Sustainable and Reliable	293
I.2	Architectural Views	293
I.2.1	Services View	294
I.2.2	Communications Architecture	298
I.3	Migration for Legacy Systems	299
I.4	Important Considerations for CI Deployers & Operators	301
I.4.1	Anticipated Changes in RLWV Environment	302
I.5	Useful References and Other Resources.....	303
I.5.1	Key Standards for System Deployment and Interoperability	303
I.6	Considerations for CI On-going Operations and Maintenance.....	304
I.6.1	Expectations for Organizational Processes.....	304

Table of Figures

Figure 1. How Standards are used in a Connected Intersection.	12
Figure 2. Connected Intersection.	13
Figure 3. Typical TSC Infrastructure Architecture.	15
Figure 4. TSC Infrastructure (with ECLA) Architecture.	16
Figure 5. Diverging Diamond.	28
Figure 6. Box Intersection.	29
Figure 7. Railroad Crossing Upstream of a Signalized Intersection.	29
Figure 8. ARC-IT Physical View.	37
Figure 9. Testing and Conformity Scope Context Diagram.	39
Figure 10. Test Methodology Concepts.	42
Figure 11. Example Test Environment for SPaT Testing.	43
Figure 12. Test Documentation Relationships.	45
Figure 13. Trajectory Error.	84
Figure 14. SPaT Information Message.	120
Figure 15. Distance and Time Elements of the TSC Infrastructure RLVW Design.	129
Figure 16. Computed Lane.	141
Figure 17. Example Next Movement State.	152
Figure 18. Example Minimum End Time, Rest in Green.	154
Figure 19. Example Next Time.	156
Figure 20. Intersection Reference Point Examples 1 and 2.	159
Figure 21. Intersection Reference Point Example 3.	159
Figure 22. Center of a Vehicle Lane.	161
Figure 23. First Node Point.	163
Figure 24. First Node Point Offsets.	165
Figure 25. Node Offsets.	166
Figure 26. Elevation Offsets.	167
Figure 27. Overlapping Ingress Lanes - Scenario 1.	169
Figure 28. Overlapping Ingress Lanes - Scenario 2.	169
Figure 29. Maximum Distance Between Node Points.	170
Figure 30. Radius of Curvature vs Distance Between Nodes.	171
Figure 31. Vertical Curves.	171
Figure 32. Lane Widths.	172
Figure 33. Example Shared Lane.	174
Figure 34. Shared Lane - Example 2.	174
Figure 35. Changes in Lane Speed Limits.	179
Figure 36. CI SPaT Message Data Structure and Content Test Case Diagram.	206
Figure 37. CI MAP Message Data Structure and Content Test Case Diagram.	207
Figure 38. CI SPaT-MAP Data Consistency Test Case Diagram.	208
Figure 39. Flow of Roadway Information in a Connected Intersection.	226
Figure 40. Security Scenario 1.	266
Figure 41. Security Scenario 2.	267
Figure 42. CI Certification Ecosystem.	268
Figure 43. CI Certification Process.	269
Figure 44. Example of Attack Tree.	270
Figure 45. Attack Tree Example - RSU Outputs Incorrect SPaT Messages.	271
Figure 46. Attack Tree Example - RSU Outputs Incorrect MAP Messages.	274
Figure 47. Attack Tree Example - RSU Outputs Incorrect RTCM Messages.	276
Figure 48. Example Testing Scope.	278
Figure 49. Example Log File Output.	279
Figure 50. Log File Entry SPaT JSON Encoding Rules.	280
Figure 51. Example Log File Entry with MAP JSON Encoding Rules.	282
Figure 52. CI System Architecture – Services View.	294
Figure 53. CI System Architecture – Communication View.	298

List of Tables

Table 1. Testing and Conformance Scope Matrix	39
Table 2. Conformance Symbols.....	48
Table 3. Conditional Status Notation	48
Table 4. Predicate Mapping	49
Table 5. Support Column Entries	49
Table 6. Needs to Requirements Traceability Matrix.....	51
Table 7. SPaT Message - Required Elements.....	132
Table 8. SPaT Message Data Sources.....	132
Table 9. MAP Message - Required Elements.....	134
Table 10. MAP Message Design Details	136
Table 11. RTCMCorrections Message - Required Elements	138
Table 12. Node Offset Ranges	164
Table 13. Radius of Curvature vs Distance Between Nodes.....	171
Table 14. Requirements to Test Case Traceability Matrix.....	201
Table 15. Mapping of J2735 Elements to TSCBM.....	222
Table 16. Example Maximum Latencies for Pathway #1 from the TSC to signal activation.	227
Table 17. Example Maximum Latencies for Pathway #2 from the TSC to the OTA Broadcast of the SPaT Message.....	227
Table 18. Required Number of RTCMCorrections Messages	248
Table 19. RTCMCorrections - Warning Distances @ 1 Hz.....	248
Table 20. RTCMCorrections - Warning Distances @ 5 Hz.....	249
Table 21. SPaT Application Security Summary	251
Table 22. SPaT SSP Octet Scheme.....	252
Table 23. SPaT Service-Specific Permissions.....	252
Table 24. SPaT Application Security Profile Identification.....	253
Table 25. SPaT Application Security Profile for Sending Messages.....	253
Table 26. SPaT Application Security Profile for Receiving Messages	254
Table 27. SPaT Application Security Management Security Profile	255
Table 28. MAP Application Security Summary	255
Table 29. MAP SSP Octet Scheme	256
Table 30. MAP Service-Specific Permissions.....	256
Table 31. MAP Broadcast Application Security Profile Identification.....	257
Table 32. MAP Application Security Profile for Sending Messages	258
Table 33. MAP Application Security Profile for Receiving Messages.....	259
Table 34. MAP Application Security Management Security Profile	260
Table 35. Signal status RTCM Application Security Summary.....	260
Table 36. RTCM SSP Octet Scheme.....	261
Table 37. RTCM Application Security Profile Identification	262
Table 38. RTCM Application Security Profile for Sending Messages.....	262
Table 39. RTCM Application Security Profile for Receiving Messages	264
Table 40. RTCM Application Security Management Security Profile	265
Table 41. Mitigations - RSU Outputs Incorrect SPaT Messages.....	273
Table 42. Mitigation - RSU Outputs Incorrect MAP Messages.....	275
Table 43. Mitigation - RSU Outputs Incorrect RTCM Messages	277
Table 44. Existing Test Documentation	278
Table 45. Services and Functionality Represented on Figure 52.	294
Table 46. Interconnections on Figure 52.	296
Table 47. Upgrade Path from Existing SPaT/MAP Broadcast Sites to the CI System.	299
Table 48. Backbone Standards.....	303

<This page intentionally left blank.>

Section 1

General Information [Informative]

1.1 Scope

This CI Implementation Guide defines the key capabilities and interfaces a connected signalized intersection must support to ensure interoperability with production vehicles for state and local IOOs. A connected intersection is defined as an infrastructure system that broadcasts SPaT, MAP, and position correction data to vehicles.

This CI Implementation Guide addresses the ambiguities and gaps identified by early deployers and provides guidance to generate messages and develop applications for signalized intersections that are interoperable across the United States, especially for automated transportation systems. This document focuses on harmonizing the existing SPaT messages deployed, using the USDOT-sponsored *Cooperative Automated Transportation Clarifications for Consistent Implementations (CCIs) To Ensure National Interoperability Connected Signalized Intersections* as a starting point.

This document was developed with the combined effort of stakeholders representing the industry at large including IOOs, Automotive Original Equipment Manufacturers (OEMs), Fleet and Truck operators, safety advocacy groups, multimodal partners, and end users of data and services. Several associations including SAE, AASHTO, NEMA, IEEE, and ITE are involved in ensuring balanced and effective stakeholder representation and adherence to consensus-based standards development process.

The CI Implementation Guide follows a Systems Engineering Process (SEP), so the contents of this document include a Concept of Operations (ConOps), a System Requirements (Functional Requirements), and System Design Details sections.

This Guide defines procurement and implementation guidance and the expectations leading to minimum performance requirements for a connected intersection. It is intended to be used by IOOs to provide guidance on how to implement an interoperable connected intersection. For OEMs and other application developers, this document provides an explanation on what data and connected vehicle messages are being provided from an interoperable connected intersection so safety applications can be developed for production vehicles, with an initial focus on the Red Light Violation Warning application. The Needs to Requirements Traceability Matrix (NRTM) in Section 3.2.3 provides the guidance to IOOs for the procurement of a connected intersection.

1.2 References

1.2.1 Normative References

Normative references contain provisions that, through references in this text, constitute provisions of this CI Implementation Guide. Other references in this document provide additional information. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this CI Implementation Guide are encouraged to investigate the possibility of applying the most recent editions of the standards listed.

Identifier	Title
ETSI TS 136 213	Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures, V14.2.0 (Release 14) [3GPP TS 36.213]
ETSI TS 136 321	Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification, V14.2.1 (Release 14) [3GPP TS 36.321]
ETSI TS 136 322	Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Link Control (RLC) protocol specification, V14.1.0 (Release 14) [3GPP TS 36.322]

Identifier	Title
IEEE Std 802.11	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, 2020.
IETF RFC 4253	The Secure Shell (SSH) Transport Layer Protocol, Internet Engineering Task Force (IETF), January 2006.
IETF RFC 8446	The Transport Layer Security (TLS) Protocol Version 1.3, Internet Engineering Task Force (IETF), August 2018.
NIST FIPS 140-2	Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, March 22, 2019. https://doi.org/10.6028/NIST.FIPS.140-2
NTCIP 1202 v03B	Object Definitions for Actuated Signal Controller (ASC) Interface, Amendment v03B, AASHTO / ITE / NEMA, published October 2023.
NTCIP 1218	Object Definitions for Roadside Units (RSUs), AASHTO / ITE / NEMA, published September 2020.
CTI 4001	Roadside Unit (RSU) Standard v01.01, AASHTO / ITE / NEMA / SAE International, September 2022.
SAE J2735	V2X Communications Message Set Dictionary, SAE International, published September 2023.
V2I Hub ICD	Integrated Vehicle-to-Infrastructure Prototype (IVP), V2I Hub Interface Control Document (ICD) - Final Report March 2017, FHWA JPO [https://usdot-carma.atlassian.net/l/c/qznaJ0DB]

1.2.2 Other References

The following documents and standards may provide the reader with a more complete understanding of connected intersections; however, these documents do not contain direct provisions that are required by the CI Implementation Guide. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on the CI Implementation Guide 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, https://arc-it.net
CCI	Cooperative Automated Transportation Clarifications for Consistent Implementations (CCIs) To Ensure National Interoperability Connected Signalized Intersections, Version 1.9.5, June 2020.
CIS Controls Guide	CIS Controls™ Implementation Guide for Industrial Control Systems, v7 https://www.cisecurity.org/white-papers/cis-controls-implementation-guide-for-industrial-control-systems/
Creation of a Guidance Document for MAP Preparation	Creation of a Guidance Document for MAP Preparation, MAP Guidance Document, Connected Vehicles Pooled Fund Study, April 2, 2021, https://virginia.box.com/v/MAPGuidanceFinal
CTI 4502	Connected Intersections Validation Report: Findings from the Connected Intersections (CI) Project Validation Phase, AASHTO, ITE, NEMA, SAE International, February 2022.
IEEE Std 610.12-1990	IEEE Standard Glossary of Software Engineering Terminology, IEEE, 1990.
IEEE Std 829-2008	IEEE Std 829 IEEE Standard for Software and System Test Documentation, IEEE, 2008.

Identifier	Title
IEEE Std 1362-1998	IEEE Guide for Information Technology System Definition - Concept of Operations (ConOps) Document, IEEE, 1998.
IEEE Std 1609.2-2022	IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages, IEEE, 2023.
IEEE Std 1609.3-2020	IEEE Standard for Wireless Access in Vehicular Environments--Networking, IEEE, 2020.
IEEE Std 1609.12-2019	IEEE Standard for Wireless Access in Vehicular Environments (WAVE)--Identifiers, IEEE, 2019.
	Enabling Connected Intersections Concept Paper – Working Draft to Support Discussions of the IOO/OEM Forum SPaT/RLVW Group.
ISO/IEC/IEEE 24765:2017	ISO/IEC/IEEE 24765:2017 Systems and software engineering- Vocabulary
ISO 26262	ISO 26262 - Road vehicles - Functional safety, International Standards Organization.
MUTCD	<i>Manual on Uniform Traffic Control Devices for Streets and Highways</i> , 2009 Edition including Revision 1 and 2 dated May 2012, Federal Highway Administration, United States Department of Transportation.
NEMA TS 2	Traffic Controller Assemblies with NTCIP Requirements—Version 03.08, NEMA, 2021.
NTCIP 9001	The NTCIP 9001, The NTCIP Guide, v04, AASHTO / ITE / NEMA, published July 2009.
RLVW Application Vehicle System, Concept of Operations	Red Light Violation Warning (RLVW) Application Vehicle System, Concept of Operations, Version 2.4, CAMP LLC, V2I-4 Consortium, 1/18/2021. https://www.campllc.org/connected-intersections-program-cip/
RLVW Application Vehicle System, High-Level System Requirements	Red Light Violation Warning (RLVW) Application Vehicle System, High-Level System Requirements, Version 1.10, CAMP LLC, V2I-4 Consortium, 1/12/21. https://www.campllc.org/connected-intersections-program-cip/
SAE J3161	LTE Vehicle-to-Everything (LTE-V2X) Deployment Profiles and Radio Parameters for Single Radio Channel Multi-Service Coexistence, SAE International, published April 2022.
SAE J3268	Listing of Provider Service Identifiers and Associated Application Technical Reports, SAE International, published March 2023.

1.2.3 Contact Information

1.2.3.1 3GPP

3GPP standards may be obtained at:

<https://www.3gpp.org/>

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

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

<https://arc-it.net>

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 CAMP Documents

CAMP (Crash Avoidance Metrics Partners LLC) documents can be accessed at the following:

<https://www.campllc.org/>

1.2.3.4 FHWA Documents

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

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

1.2.3.5 IEEE Standards

IEEE standards can be purchased online in electronic format or printed copy from the following:

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

1.2.3.6 Internet Documents

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

www.rfc-editor.org
<https://www.rfc-editor.org/retrieve/>

1.2.3.7 ITE Standards

Copies of ITE standards may be obtained from:

Institute of Transportation Engineers
1627 Eye Street, NW, Suite 550
Washington, DC 20006
(202) 785-0060
www.ite.org/technical-resources/

1.2.3.8 NTCIP Standards

Copies of NTCIP standards may be obtained from the following:

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

1.2.3.9 SAE International Documents

Copies of SAE International documents may be obtained from the following:

1.3 Terms

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

Term	Definition
Approach Speed	The uninterrupted speed (or free-flow speed) of through movement vehicles used in the design of the timing parameters that control the operations of the traffic signal.
Assured Green End Time (AGET)	AGET is the UTC time denoting the end of a green signal indication for a through movement. It is used when it can be determined with a by the CI/TSC infrastructure. It means that green indication will end unless there is preemption, failure, or something else outside of the CI/TSC infrastructure's control.
Assured Green Period (AGP)	When a connected vehicle is approaching a CI in a through lane currently in a green signal state indication, the AGP is the portion of green interval for the through movement that, when combined with the duration of the yellow change interval, decreases the likelihood that the vehicle will be in the CI during a red signal state indication.
Connected Intersections (CI)	An infrastructure system that broadcasts signal, phase, and timing (SPaT), mapping information and position correction data to On-Board Units and Mobile Units.
Connection	In the context of a connected intersection, the link between an ingress lane and a downstream lane, which may be an egress lane out of the intersection or an ingress lane within the intersection (e.g., storage lane).
Interchangeability	The capability to exchange devices of the same type on the same communications channel and have those devices interact with other devices of the same type using standards-based functions. Source: <i>NTCIP 9001</i>
Interface	A shared boundary across which information is passed. Source: <i>IEEE Std 610.12-1990</i>
Interoperability	The ability of two or more systems or components to exchange information and to use the information that has been exchanged. Source: <i>IEEE Std 610.12-1990</i>
Intersection or Intersection Box	The portion of the pavement defined from the leading edge of the stop bar to the downstream edge of the stop bar of opposing approach. The stopbars are part of the intersection box.

Term	Definition
Mobile Unit (MU)	<p>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.</p> <p>Source: <i>CTI 4001</i></p>
Movement	<p>A specific maneuver through the intersection, represented by an ingress lane and a maneuver type, such as a left turn, through, right turn, U-turn.</p>
On-Board Units (OBU)	<p>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).”</p> <p>Source: <i>CTI 4001</i></p>
Permissive movement	<p>A permitted movement that may conflict with protected movements and other permissive movements. Traffic making a permissive movement must yield to conflicting traffic and may be required to first come to a full stop.</p>
Protected movement	<p>A permitted movement that has the right of way and may conflict with permissive movements. Traffic making a protected movement must watch for conflicting traffic.</p>
Provider Service Identifier	<p>An identifier of an application area.</p> <p>Source: <i>IEEE Std 1609.12-2019</i></p>
RLVW Critical Time (RCT)	<p>The time required to traverse the length of the RLVW Detection Zone, the stopping distance to the stop line and the distance to clear the intersection.</p>
RLVW Detection Zone (RDZ)	<p>The area on a through movement lane that is used to detect vehicles for the RLVW operation. The RDZ is upstream from and adjacent to the stopping distance to the stop line with a width equal to that of the lane and a length equal to $0.5s * \text{approach speed}$.</p>
Roadside Unit (RSU)	<p>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.</p> <p>Note: Devices that are not part of the transportation infrastructure, such as cellular base stations or satellites, are not RSUs.</p> <p>Source: <i>CTI 4001</i></p>
Robustness	<p>Degree to which a system or component can function correctly in the presence of invalid inputs or stressful environmental conditions.</p> <p>Source: <i>ISO/IEC/IEEE 24765:2017 Systems and software engineering-Vocabulary</i></p>
Signal Group	<p>Data element in a SPaT message that represents traffic signal heads that control a movement of vehicles at an intersection. See Movement above.</p>

Term	Definition
Transportation Field Devices	Devices and electronic systems that monitor and control traffic operations on a roadway. Examples include a traffic signal controller and a roadside unit.
TSC infrastructure	The architectures and components within the Transportation Field Cabinet, including an external control local application (ECLA) that may assert a higher-level control over the traffic controller.
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. Source: <i>CTI 4001</i>

1.4 Abbreviations

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

AASHTO	American Association of State Highway Transportation Officials
AGET	Assured Green End Time
AGP	Assured Green Period
ARC-IT	Architecture Reference for Cooperative and Intelligent Transportation
CAT	Cooperative Automated Transportation Coalition
CCI	Clarifications for Consistent Implementations (document)
CI	Connected Intersection
ConOps	Concept of Operations
CORS	Continuously Operating Reference Station
CV	Connected Vehicle
CVPFS	Connected Vehicle Pooled Fund Study
DSRC	Dedicated Short Range Communication
DTLS	Datagram Transport Layer Security
ECLA	External Control Local Application
FCC	Federal Communications Commission
FHWA	Federal Highway Administration
FO	Functional Object
GNSS	Global Navigation Satellite System
HSM	Hardware Security Module
IEEE	Institute of Electrical and Electronics Engineers
IOO	Infrastructure Owner/Operator
ITE	Institute of Transportation Engineers

MPH	miles per hour
MU	Mobile Units
MUTCD	Manual of Uniform Traffic Control Devices
NEMA	National Electrical Manufacturers Associations
NRTM	Needs to Requirements Traceability Matrix
NTRIP	Network Transport of RTCM via Internet Protocol
O&M	Operations & Maintenance
OBU	On-Board Units
OEM	Automotive Original Equipment Manufacturers
PER	Packet Error Rate
PPP	Precise Point Positioning
PSID	Provider Service Identifier
RA	Registration Authority
RLVW	Red Light Violation Warning
RSU	RoadSide Unit
RTCM	Radio Technical Commission for Maritime Services
RTK	Real-Time Kinematic
RTM	Requirements Traceability Matrix
SAE	SAE International
SCMS	Security Credentials Management System
SDO	Standards Development Organizations
SEP	Systems Engineering Process
SPaT	Signal Phase and Timing
TLS	Transport Layer Security
TMS	Traffic Management System
TSC	Traffic Signal Controller
TSCBM	Traffic Signal Controller Broadcast Message
USDOT	United States Department of Transportation
V2I	Vehicle-to-Infrastructure
VRU	Vulnerable Road User

Section 2 Concept of Operations [Normative]

Section 2 defines the user needs that subsequent sections this CI Implementation Guide addresses. Accepted system engineering processes detail that requirements should only be developed to fulfill well-defined user needs. The first stage in this process is to identify the ways in which the system is intended to be used. In the case of the CI Implementation Guide, this first stage entails identifying the various ways in which the IOOs may provide and Automotive OEMs may use SPaT, MAP, and positioning data at a connected intersection in a consistent, interoperable manner.

This concept of operations provides the reader with the following:

- a) A detailed description of the scope of the CI Implementation Guide document;
- b) Identifies the key capabilities and interfaces for a connected intersection;
- c) An understanding of the perspective of the developers of this document; and
- d) A testing framework to verify conformance to the CI Implementation Guide.

Section 2 is intended for all readers and users of the CI Implementation Guide, including the following:

- a) **Transportation Managers.** IOO personnel responsible for making decisions about operational strategies to implement and configuring transportation field devices.
- b) **Transportation Operators.** IOO personnel responsible for monitoring the transportation infrastructure and implementing transportation strategies.
- c) **Transportation Engineers.** IOO personnel responsible for planning or designing the transportation infrastructure.
- d) **Maintenance Personnel.** IOO personnel responsible for ensuring that transportation field devices operate as intended.
- e) **Third-party data providers.** Non-IOO entities that provide SPaT and maintain SPaT and MAP data.
- f) **System Integrators.** Entities that bring together different components or subsystems into a whole system that functions together.
- g) **Application Developers.** Developers providing applications that run on on-board units (OBUs), Mobile Units (MUs), Roadside Units (RSUs) and transportation field devices; and custom applications that run from a central server, cloud service, or back-office location.
- h) **Testers.** Entities that develop test procedures to verify the SPaT, MAP, and positioning data is consistently and reliably provided by IOOs, and properly used by applications.

For the first five categories of readers, Section 2 is useful to understand what SPaT, MAP, and positioning data should be provided.

For the last three categories of readers, Section 2 provides a more thorough understanding as to why the more detailed requirements exist later in the CI Implementation Guide, and how SPaT and MAP data is derived.

2.1 Tutorial [Informative]

A concept of operations describes a proposed system from the users' perspective. Typically, a concept of operations is used to ensure that system developers understand the users' needs. Within the context of this CI Implementation Guide, the concept of operations documents the intent of each feature that a connected intersection provides.

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. This entire ConOps section is Normative unless otherwise indicated.

The concept of operations starts with a discussion of the current situation and issues that have led to the need to deploy connected intersections, and then led to the development of this Implementation Guide. This discussion is presented in layman's terms such that both the potential users of the system and the system developers can understand and appreciate the situation.

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

- **Reference Physical Architecture [Informative].** The reference physical architecture (view) defines the overall context of the connected intersection system and defines what components and interfaces are addressed by this CI Implementation Guide. The reference physical architecture is supplemented with one or more samples that describe how the reference physical architecture may be realized in an actual deployment.
- **Needs.** The needs identify and describe the various functions that users want components of the CI to perform. These needs, also called features, are derived from the high-level user needs identified in the problem statement (Section 2.2) but are refined and organized into a more manageable structure that forms the basis of the traceability tables contained in Section 3.
- **Operational Scenarios.** The operational scenarios allow a reader to understand the different parts of the proposed functions of the CI and how they interact; and may highlight situations where an ambiguity or gap currently exists among deployed connected intersections and/or current standards.

The other sections of this ConOps are as follows:

- **Operational Policies and Constraints.** A narrative description of specific policies or constraints relative to the operational environment that have a direct impact on the implementation of this CI Implementation Guide.
- **Relationship to the ITS National Architecture [Informative].** This section describes how a CI implementation fits into the ITS National Architecture.
- **Testing and Conformity Verification Management.** This section describes the need for a testing framework to verify that an implementation conforms to the CI Implementation Guide.

Section 3 Requirements uses the needs, also called features, identified in the analysis of the system to define the various requirements for a CI. Each user need traces to one or more requirements, and each requirement is derived from at least one need. This traceability is documented in a needs to requirements traceability matrix (NRTM) where each user need will map to all the requirements that fulfill that need.

Like user needs, the requirements are identified by a collaboration of a broad base of stakeholders and some are drawn from existing documents. Each requirement is captured in Section 3 Requirements in a formal manner along with the rationale which justifies the inclusion of the need. Each requirement identified is then presented in the Requirements Traceability Matrix (RTM) in Section 4.2.3, which defines how the requirement is fulfilled.

2.2 Current Situation and Problem Statement [Informative]

CIs are defined as an infrastructure **system** equipped to broadcast SPaT information message, mapping information and position correction data to support safety applications on OBUs/MUs.

CIs are being deployed as part of USDOT's Connected Vehicle Pilots program and as part of the United States' National Connected Vehicle SPaT Deployment Challenge. The SPaT Challenge was issued to state and local public sector transportation IOOs in 2017 to deploy infrastructure that broadcasts SPaT information message. The SPaT Challenge provided IOOs with an entry point to deploying a connected

vehicle infrastructure, allowing those IOOs to gain experience in procuring, installing, and operating vehicle-to-infrastructure (V2I) deployments.

Early deployments of CIs demonstrated there are issues related to providing infrastructure data in a consistent manner that will be compatible with production vehicles and in-vehicle devices. The Cooperative Automated Transportation (CAT) Coalition identified the Red Light Violation Warning (RLVW) application as one of three critical focus areas. The USDOT-sponsored CAT Coalition *Clarifications for Consistent Implementations (CCIs) To Ensure National Interoperability - Connected Signalized Intersections (CCI)* document states the following:

"It is understood by deployers that the established standards alone will not ensure open compatibility with production vehicles. Existing standards often include optional elements or flexibility given the variety of objectives or ways a system may be deployed. In some cases, the optional elements or flexibility may be interpreted differently for different deployments, despite the common objectives and applications of each deployment. These differences could lead to a lack of interoperability that prevents vehicles from using data at Connected Signalized Intersections across different jurisdictions.

Infrastructure Owner Operators (IOOs) and original equipment manufacturers (OEMs) need to reach common agreement on interpretations and clarifications regarding known ambiguities so that data from all Connected Signalized Intersections can support vehicle applications, regardless of the jurisdiction or vehicle type."

The *CCI* document then identifies and addresses known ambiguities for both mandatory and optional elements for a CI. However, the *CCI* represents only a subset (a single application - RLVW) of potential problems with implementing a connected vehicle environment.

Figure 1 is a depiction of how IOOs use standards today, and the process issues IOOs encounter that could prevent national interoperability for a CI.

STANDARDS AND HOW WE USE THEM

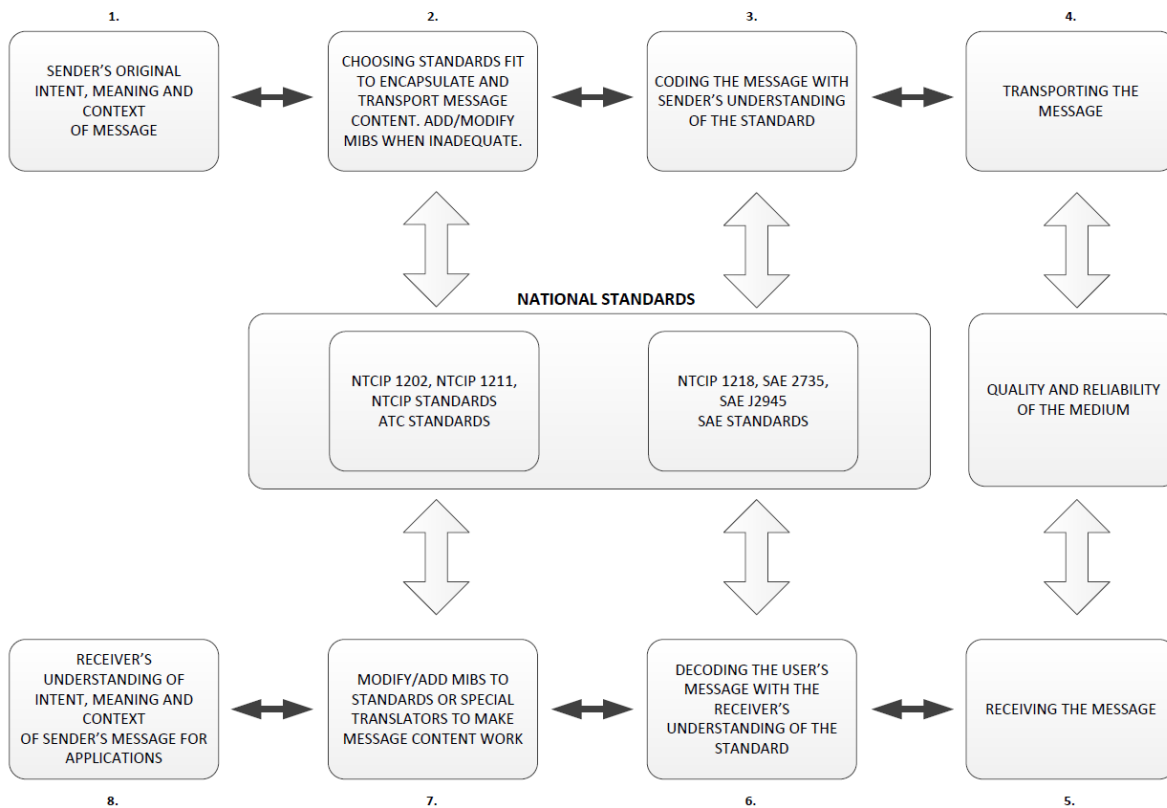


Figure 1. How Standards are used in a Connected Intersection.

The sender collects data such as real time signal status from traffic signal controllers.

To share real time signal status data from traffic signal controllers with other devices, the sender must choose a national transportation standard(s) that supports messages that can be used to send this data, such as NTCIP 1202 v03A. The sender must encode the data into the messages as specified by the selected standard, packaging all the data to be sent into the message for transporting to the receiver. The sender may modify the message by adding some objects that are not specified in the standard. This may be necessary to communicate all the data in the original context the sender wishes to send the data with. For example, traffic signal controllers designed for NTCIP 1202 v02 require custom objects to support connected vehicle applications. In a similar way, the national transportation standard selected by the computing device may contain options. The computing device may select one option and create the message in that way, while the receiver may expect or understand the message in the context of the other option.

Upon receiving the message, the receiver must decode the message and extract the original data. The sender and receiver may interpret standards differently. Unless the sender and receiver have a mutual agreement, the receiver may interpret the message differently than the sender and may not understand the original context the sender sent the data with. Additionally, in the event that the message is sent though an unreliable, poor quality medium, the message may lose some data but the receiver may not be aware of the lost data and the original context of the message. Without understanding the original context of the message, the receiver's system may not respond to the message as it otherwise would. A receiver may also receive the same type of message from other sender, but each sender may send messages with different context and the receiver would have to interpret the messages differently.

This situation is exacerbated in a situation such as a CI, where the sender and receiver are from different industries - the IOOs responsible for operating and maintaining the transportation system; and the automotive OEMs that use the transportation system.

The difference between the sender's original context of the message and the receiver's interpretation of the message, and the choices of options results in ambiguities that this CI Implementation Guide is meant to address.

2.3 Reference Physical Architecture [Informative]

2.3.1 Connected Intersection Architecture

This section presents an overview of what a complete CI "system" may look like for users of the CI, including the IOO that operates and maintains the infrastructure, and travelers through the CI. The section describes the "actors" that participate in the CI, including the producers and consumers of information, and are addressed by this CI Implementation Guide. Figure 2 is a graphical depiction (context diagram) of the physical architecture for the CI.

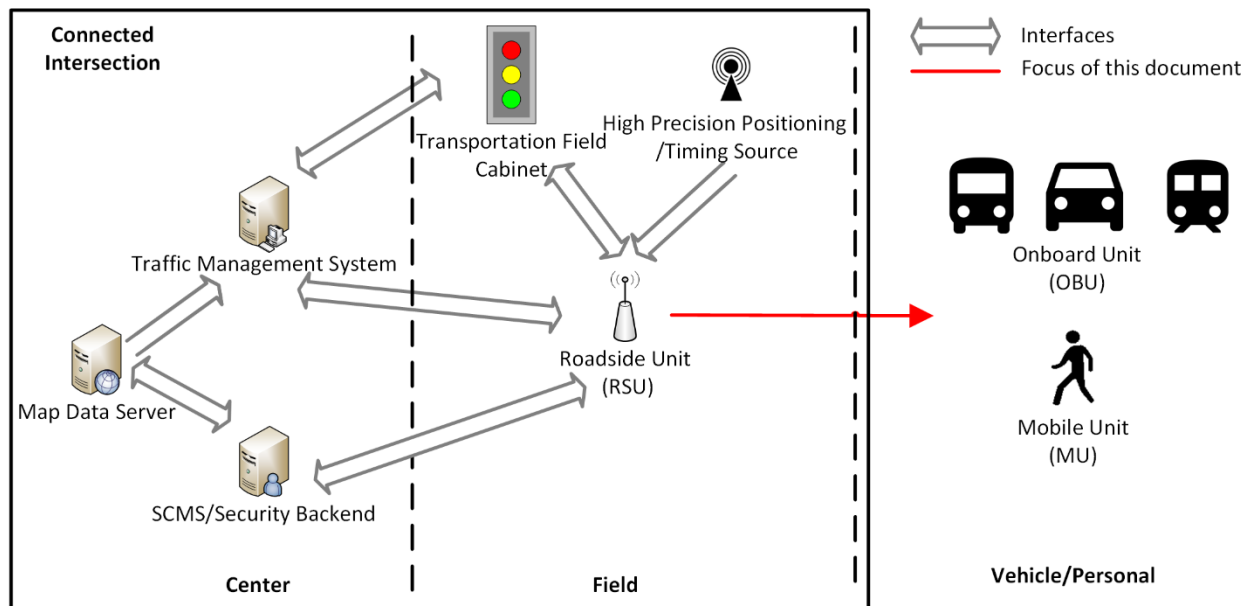


Figure 2. Connected Intersection.

At the highest level of abstraction, the physical architecture consists of center components, field components, vehicle components and personal components. The Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) defines these components as the following:

- **Center.** An entity that provides application, management, administrative, and support functions from a fixed location not in proximity to the road network. The terms "back office" and "center" are used interchangeably. Center is traditionally a transportation-focused term, evoking management centers to support transportation needs, while back office generally refers to commercial applications.
- **Field.** These are intelligent infrastructure distributed near or along the transportation network which perform surveillance (e.g., traffic detectors, cameras), traffic control (e.g., traffic signal controllers), information provision (e.g., dynamic message signs) and local transaction (e.g., tolling, parking) functions. Typically, their operation is governed by transportation management functions running in back offices. Field also includes RSU and other non-Dedicated Short Range Communication (DSRC) wireless communications infrastructure that provides communications between mobile elements and fixed infrastructure.

- **Personal.** Equipment used by travelers to access transportation services pre-trip and en route. This includes mobile/handheld as well as desktop equipment owned and operated by the traveler.
- **Vehicle.** Vehicles, including driver information and safety systems applicable to all vehicle types.

The physical elements involved are described below.

- **Traffic Management System (TMS).** The systems used by traffic operations staff to configure, control, monitor, and collect data from transportation field devices to manage traffic.
- **SCMS/Security Backend.** A system that provides and manages security certificates to support trust within the CI system.
- **Map Data Server.** A server that contains the roadway geometry data that may be shared by the infrastructure to OBUs/MUs.
- **Roadside Unit (RSU).** A transportation field device that performs the data exchange between OBUs, MUs, and other infrastructure elements.
- **Transportation Field Cabinet.** A field cabinet containing devices and electronic systems that monitor and control traffic operations on a roadway. Includes the traffic signal controllers (TSC) that allow different conflicting movements to travel across a roadway in a safe, orderly manner.
- **High Precision Positioning/Timing Source.** Source data service which could be a base station or a satellite allowing the system to calculate positioning and time for system processes, or provide position corrections. An example of a High Precision Positioning/Timing Source is a Global Navigation Satellite System (GNSS) receiver.
- **On-Board Unit (OBU).** Performs the data exchange between the infrastructure and a vehicle and installed in a vehicle (includes an after-market device). An OBU may contain applications that process the data received from the infrastructure and other sources such as another OBU.
- **Mobile Unit (MU).** Performs the data exchange between the infrastructure and a road user. MUs may be integrated with cellular phones or otherwise be carried by pedestrians, cyclists, other travelers, or workers in the roadway.

The lines between the physical elements represents the interfaces that are addressed by the CI Implementation Guide, primarily for security reasons, although the focus is on the interface between the connected intersection, specifically the RSU and the applications on the OBUs/MUs. Interfaces within the CI are shown primarily for security reasons. Other interfaces may exist among the components outside a connected intersection, such as between the Security Credentials Management System (SCMS)/Security Backend and the OBU/MU, but are not depicted in the diagram since those interfaces are not addressed in this CI Implementation Guide.

This initial CI Implementation Guide prioritizes support for the RLVW application so OEMs can begin to deploy and validate this application in production vehicles. The RLVW application is described in more detail in the RLVW Operational Scenario in Section 2.6.1. However, needs for other SPaT-based and MAP-based safety applications, that were considered relatively easy to implement and could be completely defined within this project’s schedule, are also included in this CI Implementation Guide.

2.3.2 TSC Infrastructure Architecture

Figure 3 and Figure 4 are graphical depictions of the typical architecture inside the Transportation Field Cabinet for control of a signalized intersection. The connections shown are logical. These architectures and components within the Transportation Field Cabinet are referred to as the TSC infrastructure. Figure 3 represents the most common architecture deployed today at signalized intersections.

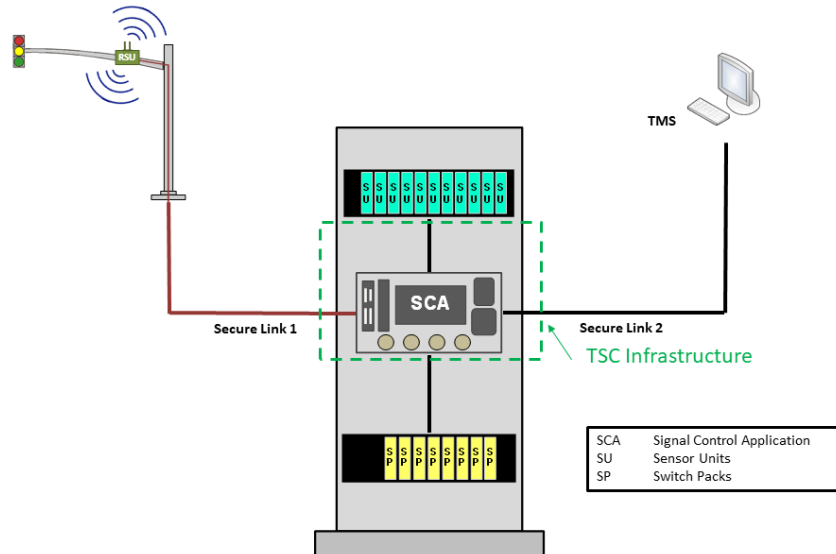


Figure 3. Typical TSC Infrastructure Architecture.

The elements involved are described below.

- **Signal Control Application.** Called the ASC Process in NTCIP 1202 v03A, represents the traditional processes providing control of a signalized intersection.
- **Sensor Units.** Called Detector Units in NTCIP 1202 v03A, devices that support the detection of travelers (e.g., vehicles, pedestrians, bicycles, transit vehicles, emergency vehicles). In some cases, the interface allows the traffic signal controller to monitor the health and gather additional information from the detection subsystems.
- **Switch Packs.** Called Load Switches in NTCIP 1202 v03A, devices used to switch power to the signal lamps/indications. This typically includes pedestrian signals, traffic signals, auxiliary signs, and other auxiliary devices.
- **Secure Link 1/Secure Link 2.** Represent the interfaces for secure data exchanges.

However, in certain cases, signal timing duration are not decided by the TSC, but rather an external control local application (ECLA) that is asserting a higher-level control over the traffic signal controller. The TSC may be commanded to run free, hold-online, or run specific coordination patterns by the ECLA that are then manipulated in real time by hold/force-off/omit or other remote commands. SPaT information messages generated by the TSC in these cases will not be accurate to the future state control commands that are offered by the ECLA. As an example, an intersection running under an ECLA to free or hold online, may not have awareness of serviceable side street demand or pending force off commands, that are being managed by the ECLA. In these cases, the ECLA must carry the responsibility to distribute the SPaT information messages since it alone knows the likely future state of the intersection. An example of an ECLA in these cases may be an adaptive algorithm application external to the TSC.

In other cases, the ECLA represents an external application or physical device that processes the signal phase and timing information from the TSC, then reformats and sends that data in a format that can be used by the RSU for broadcast to OBUs/MUs. Examples of an ECLA in these cases are the MultiModal Intelligent Traffic Signal Systems (MMITSS) and the V2X Hub.

Figure 4 illustrates how the ECLA fits in the TSC infrastructure. This figure shows a secure link between the ECLA and the RSU, the TSC, and the TMS.

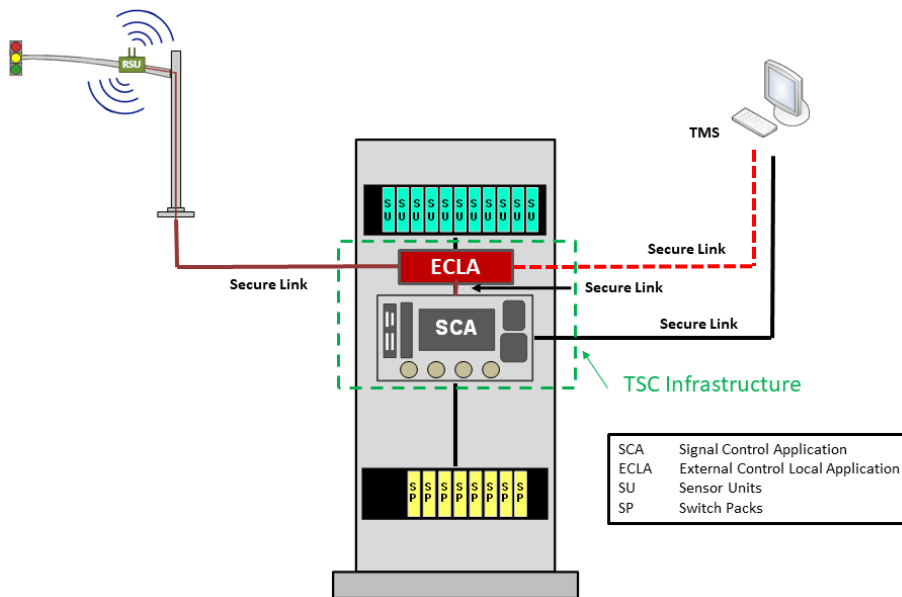


Figure 4. TSC Infrastructure (with ECLA) Architecture.

2.4 Needs

The needs for a connected intersection follow.

2.4.1 Architectural Needs

A connected intersection needs to use a communications technology to exchange data with the applications on an OBU/MU in a timely manner. This feature allows an application on an OBU/MU to receive data, such as signal timing information, with enough low latency so the application can properly process the data from the CI and react to the dynamic situation at the intersection. The reaction may include providing warnings or alerts to the driver or Vulnerable Road Users (VRUs), or taking an appropriate action.

2.4.2 Traffic Signal Controller Infrastructure Data

The traffic signal controller (TSC) infrastructure provides and serves as the source for the signal phase and timing information to the RSU and receives vehicle information from the RSU. The TSC infrastructure needs follow.

2.4.2.1 Provide Signal Timing Data to an RSU

A TSC infrastructure needs to provide signal timing data to an RSU so the RSU can forward that information to OBUs/MUs.

2.4.2.2 Provide Signal Timing Status to an RSU

A TSC infrastructure needs to provide signal timing status to an RSU so the RSU can forward that information to OBUs/MUs.

2.4.2.3 RLVW Support

The connected intersection needs to provide the CI/TSC infrastructure information necessary to enable the RLVW application as described in Section 2.6.1, Red Light Violation Warning (RLVW) Application.

The RLVW application decreases the likelihood that the vehicle will be in the intersection during a red signal indication and has the potential to reduce collisions at signalized intersection.

2.4.2.4 Receive Approaching Vehicle Information from an RSU

A TSC infrastructure needs to receive validated information from an RSU to determine the presence of an approaching vehicle. This enables the TSC infrastructure to support the RLVW application.

2.4.3 Messages

This section identifies needs related to a connected intersection providing information from the infrastructure.

2.4.3.1 Message Performance Needs

This section identifies performance needs for a connected intersection providing information from the infrastructure.

2.4.3.1.1 Uniform

A connected intersection needs to provide a consistent (or uniform) representation of the situation and operating conditions. Uniform data fields increase interoperability between the infrastructure components and the applications that use the data to aid drivers and VRUs.

For example, connected intersections should provide a uniform representation of roadway features. Inconsistencies in how roadway features are represented lead to inconsistent usage and interpretations by applications that use roadway features. A uniform representation of roadway features increases the effectiveness of the applications that aid drivers and vulnerable road users.

2.4.3.1.2 Robustness

A connected intersection needs to be robust. When subject to anomalous data and commands, the connected intersection and its components function properly and are not corrupted. These components may have different failure modes operational states that are consistent and repeatable under different operational conditions. An example is what data should still be broadcasted if the connected intersection is unable to provide the current movement state.

The connected intersection and its components also function properly under the maximum simultaneous data traffic possible on all communications interfaces. Applications depend on continuous and proper operation under extreme demands on the system.

2.4.3.1.3 Concise Messages

A connected intersection needs to provide concise messages so that complete data describing the situation can fit within the maximum message size supported by the communications stack. Small message sizes also suffer less from packet loss than larger messages.

2.4.3.1.4 Advanced Notification

A connected intersection needs to provide data far enough in advance of the intersection with respect to both time and distance so the application on an OBU/MU can process the data in time to react to a situation. This allows the proper interpretation of the data by the applications and may provide more options for drivers, VRUs or applications to react to the dynamic situation at the intersection. The reaction may involve providing warnings or alerts to the driver or VRU, or taking an appropriate action. For example, the coverage area needed will be different for a CI where average vehicle approach speeds are

20 miles per hour (MPH) when compared to a CI where the average vehicle speed for an approach is 50 mph.

2.4.3.1.5 Timeliness

A connected intersection needs to indicate changes in state and timing within a specified latency constraint so that the applications on an OBU/MU can react to the most current information in a timely manner. Timely information to applications provides effective and reliable services that aid road users.

2.4.3.1.6 Quality Assurance

The CI needs to produce quality information. The information needs to produce the best set of messages (e.g., SPaT message) that represents the current situation and conditions at the intersection.

2.4.3.2 Generic Message Data Needs

This section identifies generic data needs for a connected intersection providing information from the infrastructure.

2.4.3.2.1 Time Source

A connected intersection needs to use the same time reference and with sufficient precision and accuracy as OBUs/MUs so non-infrastructure applications can properly interpret time points. This allows the proper interpretation of time-sensitive data by applications and permits reactions to be based on the same understanding of time.

2.4.3.2.2 Message Revision

A connected intersection needs to indicate if the data provided on a specific topic (other than the timestamp) is new. This allows the receiving application to make a determination as to whether it should process the data.

2.4.3.2.3 Timestamp

A connected intersection needs to identify the time that the data provided by the infrastructure was generated. This allows an application using the same time source to determine the timeliness of the data.

2.4.3.3 Signal Timing Data Needs

This section identifies needs related to signal timing data that a connected intersection provides.

2.4.3.3.1 Intersection Identification

A connected intersection needs to provide the unique identifier of an intersection so an application can associate the signal timing data received with the intersection map data.

2.4.3.3.2 Intersection Status

A connected intersection needs to provide information about the current operational status of a signalized intersection so that an OBU/MU application can better interpret signal timing data provided about that intersection.

For example, the operational status may indicate if the signalized intersection is operating in preempt, external logic, or in flash.

2.4.3.3.3 Current Movement State

A connected intersection needs to provide information about the current state of each movement—including a pedestrian movement—at the intersection so an application can provide the proper warnings, information, or guidance to the driver or VRU. The current state identifies if a maneuver through an intersection is currently allowed and any restrictions. For example, the current state may indicate whether a protected or permissive movement is allowed, a protected or permissive clearance (phase change interval) is in effect, the movement is required to stop then proceed, remain, or a movement may proceed with caution with possible conflicting traffic.

2.4.3.3.4 Next Movement State

A connected intersection needs to provide information about the next state of each movement at the intersection so an application can provide the proper warnings, information, or guidance to the driver or VRU. The next state identifies if the next signal interval for a maneuver through an intersection will be allowed and any restrictions after a change. For example, the current state may indicate a protected or permissive movement, but the next state indicates when the current state changes, if the maneuver will change to a protected or permissive movement, or a clearance (e.g., yellow indication) interval will be in effect.

2.4.3.3.5 Time Change Details

A connected intersection needs to provide information about when the current signal interval (state) for each movement, including a pedestrian interval (state), at the intersection will change so an application can provide the proper warnings, information or guidance to the driver or VRU. The information provided must be accurate under all conditions such as during TSP (transit signal priority) and EVP (emergency vehicle preemption).

The need includes the following operational scenarios: 2.6.2.1 - Rest in Green.

2.4.3.3.6 Next Allowed Movement Time

A connected intersection needs to provide the estimated time when each movement at an intersection is next allowed to proceed (e.g., green or flashing yellow), excluding unexpected events such as a preemption request. This feature allows an application to provide information or guidance to a driver or VRU. The next allowed-to-move information partially satisfies the needs of an eco-driving application.

The next allowed-to-move information also helps an OBU/MU determine whether a permissive turn movement will change directly to a protected movement, will change to a protected movement after a clearance interval, or will change to a stop condition after a clearance interval.

2.4.3.3.7 Enabled Lanes

A connected intersection needs to provide information about which revocable lanes are currently enabled so an application can determine what movements are currently allowed at an intersection. An IOO may define the same physical lane for different uses or with different restrictions depending on the time of day or on specific days. For example, a lane may be defined as an HOV lane during the morning rush hours, a reversible lane for special events (such as at an arena), and as a normal vehicle lane during all other times. This feature allows the connected intersection to indicate what restrictions are in effect.

2.4.3.3.8 Signal Timing and Roadway Indications Synchronization

A connected intersection needs to provide signal timing data that is synchronized with signal indication changes on the roadway within a defined tolerance. For safety and effectiveness, applications require consistency between the perceived state of the intersection by road users and the signal timing data

received by the applications on an OBU/MU. Synchronization enables applications to safely and effectively provide services to road users.

For example, the duration of a signal interval may be influenced by external processes. There are configurations when an external process, such as cabinet relays or a separate system controlling the active timing intervals (e.g., hold/force off/stop time), is being used for either supervisory control over the traffic controller timing or post processing of controller outputs. In these cases, the traffic controller may have limited information thereby limiting the ability to predict the future state of the intersection and therefore cannot provide accurate signal interval duration information. For these cases, the source of the signal interval duration data should be the separate system.

2.4.3.4 Roadway Geometry Data Needs

This section identifies needs about the roadway geometry information that a connected intersection provides.

2.4.3.4.1 Intersection Geometry

A connected intersection needs to provide information about the lanes in and around an intersection so that an application on an OBU/MU can determine its position in relation to the lanes, stop lines, crosswalks and landing geometry of the intersection.

2.4.3.4.2 Lane Attributes

A connected intersection needs to provide information about the allowed use of each lane at an intersection so an application on an OBU/MU can determine the current allowed usage of the lanes around its position and can provide appropriate warnings, information and guidance to the driver or VRU. Lane attributes provided include the direction of travel permitted in the lane and lane use restrictions.

2.4.3.4.3 Allowed Maneuvers

A connected intersection needs to provide information about the allowed maneuvers of each lane at an intersection so the application on an OBU/MU can provide appropriate warnings, information and guidance to the driver or VRU. Allowed maneuvers define permitted turns from a lane, typically a vehicle lane, under different conditions.

2.4.3.4.4 Connections Between Lanes

A connected intersection needs to provide information about the permitted connections between ingress lanes and egress lanes at an intersection so an application on an OBU/MU can determine what signal timing data from the infrastructure applies to it. The application uses this information to provide appropriate warnings, information and guidance to the driver or VRU.

For example, this need ties a maneuver to a signal group so the application on an OBU can interpret what signal timing data applies.

2.4.3.4.5 Approach Speed Limit Information

A connected intersection needs to provide the posted or statutory speed limit, whichever is applicable, for each lane so an application in an OBU can provide advisories or warnings to a driver based on the speed limit.

2.4.3.4.6 Revocable Lanes

A connected intersection needs to identify lanes that are revocable. An IOO may define the same physical lane for different uses or with different restrictions depending on the time of day or on specific

days. For example, a lane may be defined as an HOV lane during the morning rush hours, a reversible lane for special events (such as at an arena), and as a normal vehicle lane during all other times.

NOTE: The SPaT message will then identify which revocable lane is currently is active.

2.4.3.4.7 Road Geometry Accuracy

A connected intersection needs to provide road geometry data within a defined accuracy and precision to represent the actual roadway geometry at the intersection. Inaccurate data reduces the effectiveness of the applications that use the data.

NOTE: Enough accuracy is needed so the vehicle can determine which lane it is in, since different lanes may be controlled by different signal indications being in different states.

2.4.3.4.8 Signal Timing and Roadway Geometry Synchronization

A connected intersection needs to ensure that roadway geometry information being broadcast reflects the current operating state used to generate the signal timing data. The signal timing data and roadway geometry data cannot be viewed as independent, but BOTH need to reflect the actual usage. The signal timing data and the operating roadway geometry HAVE to be agreement. If an entity changes the design geometry environment, it may necessitate a change in the signal timing data.

2.4.3.5 Positioning Data Needs

This section identifies needs about positioning that a connected intersection provides.

2.4.3.5.1 Positioning Corrections Data Format

A connected intersection needs to provide GNSS corrections data in a standardized format that helps vehicles achieve the required positioning and timing accuracy. This enables vehicles to use a common representation of GNSS corrections data at any connected intersection where corrections data is available.

2.4.3.5.2 Real-Time Kinematic Corrections

RSUs at connected intersections need to broadcast the appropriate Real-Time Kinematic (RTK) corrections messages to OBU/MU devices for achieving lane-level vehicle positioning. This improves positioning accuracy and the performance of RLVW and other safety applications.

Note: OBU/MUs can receive corrections information from other sources (e.g., cellular networks), which is out of scope of CTI 4501. OBU/MUs in OEM vehicles often have access to alternative precision positioning methods.

2.4.4 Security

This section identifies security needs for a connected intersection.

2.4.4.1 Correct Operations

This section identifies the security needs for correct operations at a connected intersection.

2.4.4.1.1 Operations - Data Trustworthiness

A connected intersection needs to ensure that data sources are trustworthy and provide correct data for use in creating CI messages so that message data reflects near-real time CI operating conditions, and applications and users respond appropriately.

2.4.4.1.2 Data Processing

A connected intersection needs to ensure that platforms that modify or perform any transformation on data that is subsequently used to create CI messages are trustworthy and operate correctly, including producing correct outputs so that transformed data reflects near-real time operating conditions, and applications and users respond appropriately.

2.4.4.1.3 Input Validation

A connected intersection needs to ensure that components reject incorrect inputs, or inputs that do not communicate appropriate levels of trustworthiness, so that components do not process data that misrepresents the CI operating environment.

2.4.4.1.4 Cyber Attacks

A connected intersection needs to ensure that all components involved in generating CI messages or inputs into CI messages are protected from cyber attacks so that malevolent actors may not gain access to or harm the CI system.

2.4.4.1.5 Cyber Attacks Recovery

A connected intersection needs to ensure that all components involved in generating CI messages or inputs into CI messages can recover from cyber attacks so that disruption due to cyber attacks is limited, allowing components to provide near-continuous CI operating environment data.

2.4.4.1.6 Resilience

A connected intersection needs to be resilient and ensure that all components operate correctly and produce correct output in the case where the CI operating environment does not meet acceptable performance conditions so that applications and user actions remain safe and appropriate during these conditions.

For example, if the time of change for a traffic controller is not reliable, the RSU may still broadcast intersection status data but not time-of-change data for a SPaT message.

2.4.4.1.7 Secure Administration

A connected intersection needs to enable components to be updated or reconfigured by appropriately authorized actors if necessary, to improve resilience / security against cyber attacks so that selected components may be modified, as appropriate. For example, if some, but not all, components are vulnerable, it may be appropriate for an authorized actor to update/reconfigure selected components to allow those that are not affected by the cyber attack to continue operation, without interruption.

2.4.4.1.8 Authenticated Secure Update

A connected intersection needs to support remote, authenticated, verified updates so that components maintain a minimum threshold of current cyber-hygiene. For example, as new cyber threats are identified, protection software is updated for all system components.

2.4.4.1.9 Assurance of Correct Network

An RSU needs to have assurance of connectivity to the network of the correct connected intersection and central system.

2.4.4.1.10 Secure Backend

A connected intersection needs to be connected to a secure backend network of the IOO to ensure that link to the center systems and field devices are protected.

2.4.4.1.11 Physical Security

A connected intersection needs to ensure that physical access to equipment involved in operating the system is limited by establishing physical security controls to reduce the possibility that a physical attack interferes with or prevents the correct operation of the system.

2.4.4.1.12 Device/System Monitoring

A connected intersection needs to have access to a system to manage security information and events to improve the detection and remediation of security issues and provide an extra layer of in-depth defense.

2.4.4.2 Data Flow: Communications and Interface Security

This section identifies the security needs related to data flow (communications and interfaces).

2.4.4.2.1 Data Flow Trustworthiness

A connected intersection needs to provide components receiving CI data with sufficient information to evaluate trustworthiness of received data so those components receive some assurance that the CI data reflect near-real time CI operating conditions, and applications and users respond appropriately.

2.4.4.2.2 Data Integrity

A connected intersection needs to ensure that CI data is not corrupted or changed as it passes across interfaces so that transformed data reflects near-real time operating conditions, and applications and users respond appropriately.

2.4.4.2.3 Data Confidentiality

A connected intersection needs to protect the data exchanged across interfaces from unauthorized access.

2.4.4.3 Network Monitoring

This section identifies the security needs for network monitoring to allow implementing mechanisms to detect faulty CI messages.

2.4.4.3.1 Misbehavior Reporting by Network Administrators

A connected intersection needs to provide a mechanism to allow IOO network administrators to detect incorrect data so that faulty CI messages do not compromise applications or user actions.

2.4.4.4 Credential Management

This section identifies the security needs for credential management.

2.4.4.4.1 Credential Provisioning

A connected intersection needs to ensure that components that send trusted information communicate using up-to-date credentials so that components establish trust with each other, as well as OBUs and MUs.

2.4.4.4.2 Management of Untrustworthy Devices

A connected intersection needs to provide a mechanism to modify the ability of any component determined to be untrustworthy to participate in the system so that untrustworthy devices do not have a negative impact on CI operations. Untrustworthy devices are:

- Devices whose integrity, reliability or availability has been determined to be compromised;
- Devices otherwise determined to not be meeting performance requirements specified for the supported applications; or
- Devices whose credentials/certificates are revoked.

This applies to devices within the connected intersections (e.g., TMS, transportation field cabinet, etc.) but not OBUs/MUs.

2.4.4.4.3 Credentialing System Access

All devices in a connected intersection supporting a RLVW system needs access to one or more sources, such as the SCMS or a credentialing system, of digital credentials specific to each supported device. This allows the RSU to verify the trustworthiness of the data.

NOTE: the OBU/MU also need access to the SCMS or a credentialing system so it can verify the messages from the connected intersection.

2.4.5 Operations and Maintenance Needs

This section identifies operational and maintenance (O&M) needs for a connected intersection.

2.4.5.1 Interoperability

A CI needs to maintain interoperability with other CI systems within the North America over an extended period of time.

2.4.5.2 Lifecycle

A CI lifecycle needs to accommodate: initial installation, security certificate provisioning, system validation and commissioning into operation, normal operations with system monitoring and anomaly detection, maintenance/degraded operation, system outages, equipment upgrades/swap-out, software/firmware updates, system revalidation following recovery or changes, and equipment removal/decommissioning.

2.4.5.3 Maintenance

A CI needs to be maintained and operated as part of the normal O&M infrastructure supported by the IOO. The CI should be managed at the level of skills and capabilities of existing resources (with some additional training, better tools, etc). Also the CI needs to be incorporated into existing IOO processes and practices which are used to maintain traffic signals and other infrastructure components including inventory management, field upgrades, field troubleshooting, system monitoring etc. O&M includes maintaining security, accuracy and accountability of operations for all of the IOO's infrastructure including the CI to meet application safety, system security and operational objectives.

2.4.5.4 System Diagnostic Interface

A connected intersection needs adequate diagnostic capabilities to report on key system performance indicators for system validation and monitoring, e.g., time tolerance, message flow, message accuracy.

2.4.5.5 System Performance Monitoring

A connected intersection needs to ensure that all components and the overall system are monitored and evaluated continuously to determine if the system is operating within specified tolerances of the expected performance. This feature allows the system to detect performance deviations and generate appropriate system exceptions and alerts.

2.4.5.6 System Upgradeability

A connected intersection needs to support upgradeability, provisioning and updates to support expected system lifecycle and evolution, such as changes in standards, firmware updates, hardware migration, etc. This feature allows the system to be updated/maintained without jeopardizing integrity and security of the messages/data transmitted to on-board units (vehicle/mobile units/etc).

2.5 Operational Policies and Constraints

The following operational policies and constraints apply to the use of this CI Implementation Guide document:

- a) The operation and maintenance of the connected signalized intersection are governed by the regulatory guidelines or policies for the operating agency (IOO) that may include USDOT's and the relevant states' *Manual of Uniform Traffic Control Devices (MUTCD)*, and state and local ordinances, policies, and procedures.
- b) The operation and maintenance of the connected signalized intersection uses the traffic signal timing principles and practices that have guided signal timing operations for many decades. Many of these principles and practices have been studied, researched, and time tested. Significant changes to these principles and practices may require additional studies and research before they can be adopted and deployed.
- c) Gaining complete nationwide uniformity in signal timing and operations may not be possible without changes in the current national governance framework. Currently, no single entity governs the operation of every traffic signal. Every state, county, and city are often responsible for their own traffic signals and may have their own approaches to signal timing and operations, within the constraints of laws and ordinances.
- d) Vehicles and vehicle systems are subject to Federal Motor Vehicles Safety Standards, *ISO 26262 – Road vehicles – Functional safety, ISO/PAS 21448:2019 – Road vehicles - Safety of the Intended Functionality*, a number of voluntary guidelines and/or non-regulated standards as well as OEM internally specified requirements and/or design principles.
- e) While developers are aware of the need for guidance that is feasible and implementable, certain technologies may not be available given resource constraints.

2.6 Operational Scenarios

According to *IEEE 1362-1998*,

"A scenario is a step-by-step description of how the proposed [system] should operate and interact with its users and its external interfaces under a given set of circumstances. Operational Scenarios help readers understand how all pieces of the system interact to provide operational capabilities. [IEEE 1362-1998]"

For the purposes of this project, the proposed system is a connected intersection or series of connected intersections as might be found along an arterial. The operational scenarios are optional for the CI Implementation Guide, but could be included if the operational scenario includes the following:

- Allows a reader to understand the different parts of the proposed functions of the CI and how they interact
- Highlights a situation where an ambiguity or gap currently exists but will be addressed by the CI

2.6.1 Red Light Violation Warning (RLVW) Application

Title	Red Light Violation Warning (RLVW) Application
Background	<p>The purpose of the RLVW application is to provide advisories, warnings, or alerts to a driver approaching a signalized CI where they are unintentionally not stopping for a red signal indication or they may not clear an intersection before the signal turns red. The goal to clear the intersection before the signal turns red is a higher operational requirement than that used with most U.S. traffic control devices where it is acceptable for a vehicle to be in an intersection when a signal turns red. The CI conveys to the on-board units and mobile units (OBUs/MUs) the minimum and maximum end times possible for the current and next signal indications for each signal group at the intersection. Therefore, there can be a range for the end time of a given signal indication.</p> <p>For the RLVW application to be effective, a RLVW-equipped vehicle requires “assured” (very high certainty) end of green signal times when it approaches CIs in a through movement. These assured green end times (AGETs) are at the highest level of certainty for the CI/TSC infrastructure that controls the right-of-way for the CI although it is possible for an AGET to be inaccurate due to preemption, a failure, or something else outside of the CI/TSC infrastructure’s control.</p> <p>There are various types of intersection control used in the United States including fixed time (pretimed), actuated signal control, traffic responsive control, adaptive control, and others. Fixed time control uses preset time intervals that are the same every cycle of the intersection, regardless of changes in traffic volumes and on-street demands for right-of-way. Fixed time control is most suitable for intersections where traffic patterns are relatively stable. If traffic volumes and patterns change predictably during the day, fixed time control can be designed to accommodate the variations. An AGET is readily identified for intersections under fixed time control since the timing of the entire intersection is known in advance.</p> <p>This is not the case for actuated signal control (and other hybrid types of traffic control). The purpose of actuated control is for intersections to be able to respond to the changes in traffic volumes and on-street demands for right-of-way. The major advantage of actuated control over fixed time control is reduced road user delay. This flexibility, however, can make providing AGETs difficult. It is common for an approach to an intersection to be programmed to “rest in green.” In this case, the minimum end time for the green approach may be 0.1 seconds and the maximum end time may be unknown. Intersection demand from a cross street could terminate the green approach in 0.1 seconds and prohibit the RLVW application from performing its safety functions.</p> <p>The CI/TSC infrastructure can mitigate this uncertainty and enable the RLVW application by providing an assured green period (AGP) as part of the green interval for the through movement. This AGP is calculated and programmed so that when it is combined with the duration of the yellow change interval, decreases the likelihood that the vehicle will be in the intersection during a red signal indication. A virtual RLVW Detection Zone (RDZ) is defined where basic safety messages (BSMs) from OBUs/MUs on vehicles are used to determine when the AGP is to be applied. When the CI/TSC infrastructure is not terminating the green and a vehicle has been detected in the RDZ, the minimum end time of the movement is set to the current time plus the AGP to facilitate the vehicle clearing the CI. When the CI/TSC infrastructure determines that the green approach is to be terminated, the CI/TSC infrastructure provides an AGET that is greater or equal to the current minimum end time. Vehicles that are in the RDZ or closer to the stop line will have already received a minimum</p>

	end time that will help them clear the intersection. Vehicles that are upstream from the RDZ will have time to stop before the stop line.
Summary of Operations	<p>The scenario for the RLVW application for a CI under actuated control is described in the following steps.</p> <ol style="list-style-type: none"> 1) Parameters used by CI/TSC infrastructure are calculated and programmed for all through movements for the intersection including the following: <ol style="list-style-type: none"> a) The approach speed; b) The distance to bring a vehicle to stop at the stop line based on the approach speed; c) The distance to clear the intersection; d) The size and position of the RLVW Detection Zone (RDZ); and e) The AGP. 2) When a RLVW-equipped connected vehicle (CV) approaches a CI, the OBU/MU receives signal timing and roadway geometry data from the CI. At the same time, the OBU/MU is sending its location data and other vehicle-related data to the CI. 3) If the CI detects a vehicle in the RDZ, the associated movement is in green, and the CI is not terminating the movement, then the CI sets the minimum end time of the movement to the current time plus the AGP. 4) If the CI determines that a movement currently in green is to terminate, the CI provides an AGET that is equal to or greater than the current minimum end time for the movement. 5) Once the CI provides the AGET, the RLVW application on the OBU/MU may provide advisories, warnings, or alerts to the driver.

2.6.2 Signal Timing Scenarios

This section identifies common signal timing operations at a signalized intersection.

2.6.2.1 Rest in Green

Title	Rest in Green
Summary of Operations	<p>The major street has a pre-defined green phase time. When this time is reached, the intersection transits to green “Rest Mode” where the major street continues in green operation until either a pedestrian actuation, a cross-street vehicle actuation, or an eventual timing out occurs.</p> <p>The connected intersection would either provide the following:</p> <ul style="list-style-type: none"> • Time change details that indicate when the current green phase will change for certain • Time change details that indicate the minimum amount of time before the current green phase will change, if the time of change cannot be determined
Need	This operational scenario leads to the needs for Assured Green End Time.

2.6.2.2 Two or More Signals or Intersections with One Controller

Title	Two or More Signals or Intersections with One Controller
Summary of Operations	<p>This operational scenario addresses a single traffic signal controller used to control two or more intersections (usually closely-spaced) or signalization of an advanced approach, driveway, or maneuver related to the main intersection. The geometry of these intersections creates some additional challenges in creating MAPs and signal groups because of distances, interior maneuvers, and additional stop line locations. In each of these cases, SPaT and MAP must be communicated consistently and accurately to prevent a vehicle from stopping on a green signal indication or running a red signal indication. Examples of uses cases in this scenario are the following:</p> <ol style="list-style-type: none"> 1) Two closely spaced intersection

- a) Texas Diamond
- b) Diverging Diamond (See Figure 5)
- 2) Box intersection (2 divided highways crossing or frontage road intersections at a 3-level diamond interchange) (See Figure 6)
- 3) Signalized driveway upstream of a signalized intersection driven by one controller to handle spillback
- 4) Railroad crossing upstream of a signalized intersection with stop line and signal head in advance of crossing driven by one controller to handle spillback (See Figure 7)
- 5) Signalized crosswalk close to the intersection
- 6) Michigan Left-Turn where the U-turn is signalized
- 7) Signalized roundabout

Graphics



Figure 5. Diverging Diamond.



Figure 6. Box Intersection.

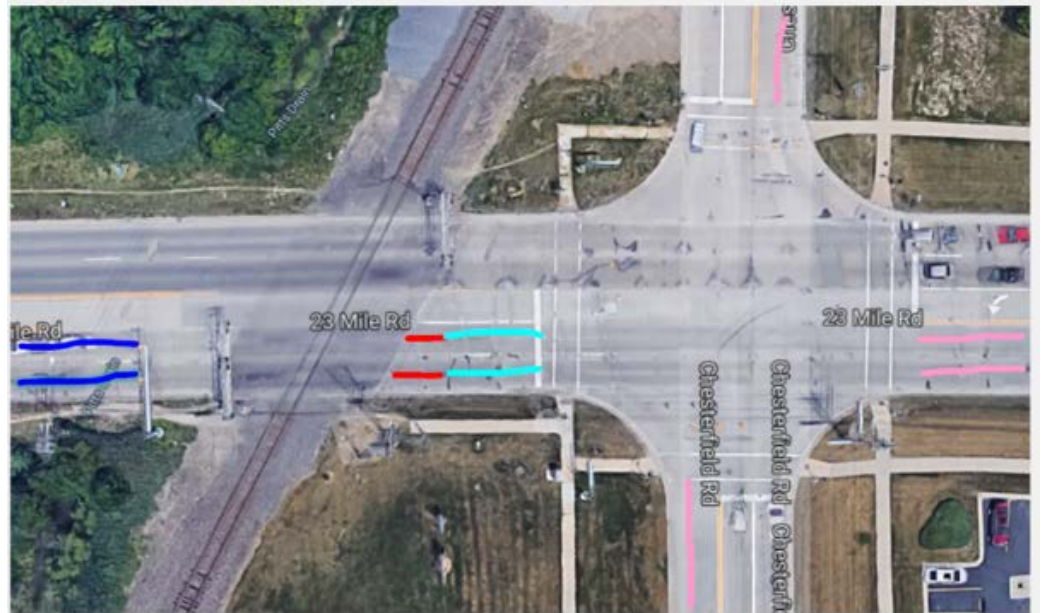
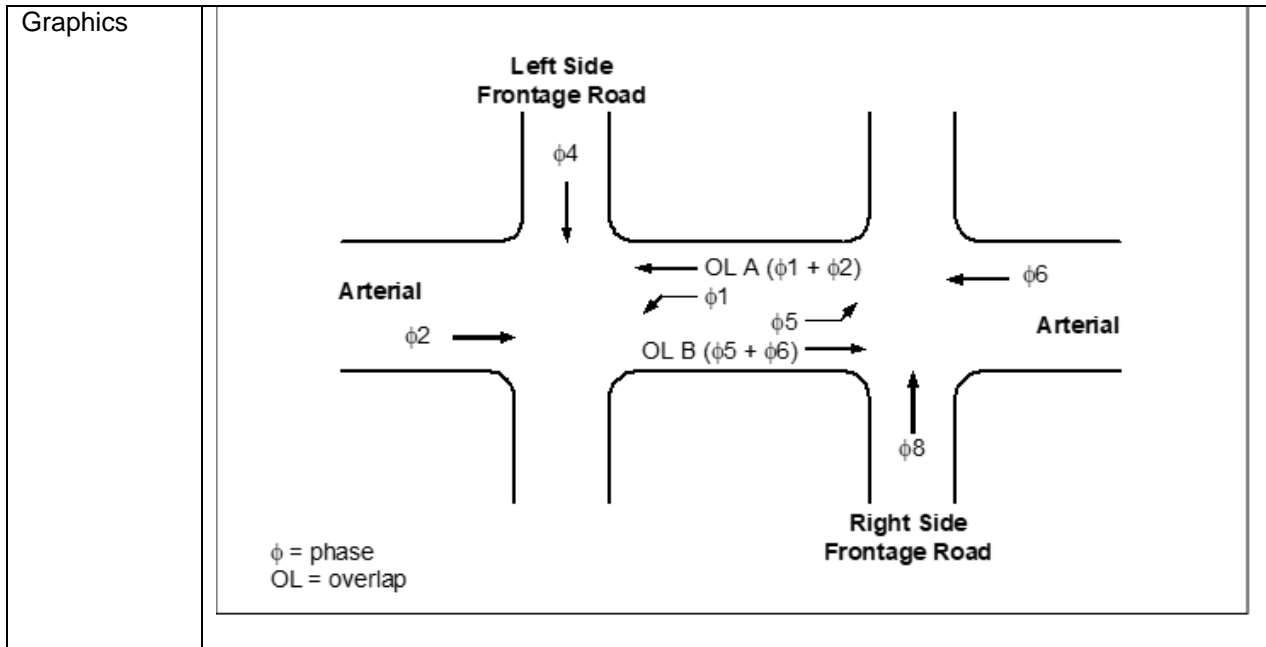


Figure 7. Railroad Crossing Upstream of a Signaled Intersection.

Source: Christopher Poe, Mixon Hill.

2.6.2.3 Texas Diamond Intersections

Title	Texas Diamond Intersections
Summary of Operations	<p>Texas Diamond Intersections also commonly known as diamond interchanges function as an interface between a freeway and a surface street. Most Texas freeways are characterized by frontage roads. The Texas Diamond is the intersection of the frontage roads with a surface street. The two frontage roads on either side of the freeway form two intersections with the surface street.</p> <p>Figure 1 illustrates a simplified version of the phasing configuration of the Texas diamond interchange. The phasing is similar to the NEMA configuration of a typical intersection and is characterized by:</p> <ul style="list-style-type: none"> • Phase 2 and Phase 6 are phases for arterial through movements similar to a typical intersection • Phase 4 and Phase 8 are phases for frontage road movements similar to through movements on a cross street • Phase 1 is a phase for an internal left turn movement that opposes Phase 2 and Phase 5 is a phase for an internal left turn movement that opposes Phase 6 • Overlap A (OL A) is an internal overlap that is ON when Phase 1 OR Phase 2 are ON • Overlap B (OL B) is an internal overlap that is ON when Phase 5 OR Phase 6 are ON <p>While diamond interchange operations are primarily impacted by the spacing between the two intersections, traffic patterns also can influence the operational strategies. The operational philosophy is to optimize external demands while ensuring that the interior does not get backed up. A diamond interchange can be operated in three sequences when operating according to TxDOT Specifications.</p> <ul style="list-style-type: none"> • Three phase - Three phase sequence is typically used when spacing between the two intersections is large (usually greater than 400 feet). The large spacing allows for storage of interior left turning vehicles that enter the interchange. • Four phase - Four phase sequence is typically used when spacing between the two intersections is small (usually less than 400 feet). The small spacing requires a phasing sequence that ensures that no vehicles stop in the interior of the interchange. • Separate intersection mode - Separate intersection mode is usually applied when the spacing between the two intersections of a diamond interchange is very large (greater than 800 feet).



Needs	<p>SPaT Message Needs Most diamond interchanges in Texas are operated using a single controller. Most of the phasing sequences use typical phases which can potentially be translated to phase groups. These phases and phase groups are very similar to the phases and phase groups for a typical intersection. Hence, it is possible for a diamond interchange to have a single SPaT message in spite of having two intersections. The SPaT information message that is unnecessary to compile a SPaT message can be generated by the traffic signal controller.</p> <p>MAP Message Needs Texas Diamonds can vary in width. Due to constraints of DSRC range, a larger number of approaches (six instead of four approaches at a typical intersection) and size of the MAP message, it might be necessary to generate the SPaT message and a separate MAP message for each side of the diamond interchange. These two MAP messages can then be broadcast using two separate RSUs located at each intersection. Each intersection will have a unique IntersectionID which can support in identifying which intersection the vehicle is approaching when a vehicle receives two MAP messages from two different RSUs.</p>
-------	---

Source: Srinivasa Sunkari, Texas A&M Transportation Institute.

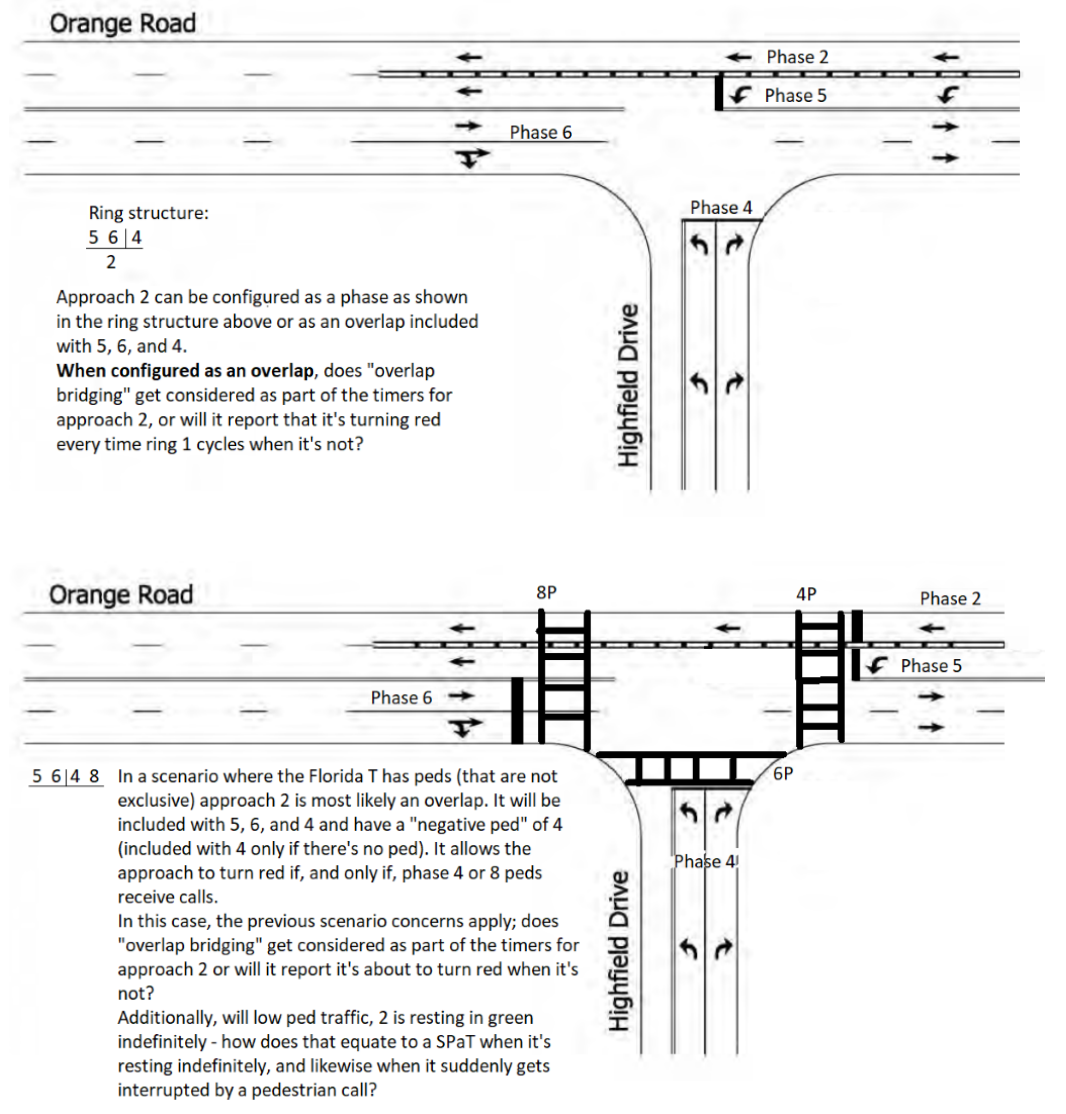
2.6.2.4 Florida T Intersection

Title	Florida T Intersection
Summary of Operations	<p>A Florida-T intersection's configuration is a step above a traditional T intersection. The Florida-T encourages safer operations by providing both deceleration and acceleration lanes for left turning vehicles.</p> <p>Florida-T intersections can also be signalized when needed to create adequate gaps in traffic for turn movements into and out of the Tleg of the intersection. Even with signalization, one direction of through traffic can continue through the intersection without stopping.</p> <p>Two examples are shown below; one with peds, one without. Each presents questions for the traffic controller issues TF on whether or not the current timing parameters account for these uncertainties/complications:</p>

Summary of considerations for this scenario include the following:

- How does a phase resting indefinitely report min time, maxtime, and likely time? Is that what a driver expects?
- Does an overlap that's constantly bridging accurately report that it will bridge when it's included phases are transitioning from one to the next?
- How does a phase that's resting indefinitely but can/will suddenly get terminated by a ped impact the timing and confidence reports?
- In cases where a controller allows a "phase next" decision to be changed past the point of yellow clearance... If an overlap is bridging (say to go from 4 to 5 in the example above), but a late ped call arrives on ped 8 – the overlap will stop bridging and terminate. This brings up two considerations for SPaT timings;
 - The controller (if in coordination) will now transition, making confidence go down
 - The phase will take longer to get to than expected because the overlap trail yellow and red needs to be served beyond its included phase clearance since it started clearing late

Graphics



Source: Whitney Nottage, Intelight.


2.6.2.5 User Logic - Outside the "Knowledge" of the Controller

Title	<p>User Logic - Outside the "knowledge" of the controller</p> <p>Note: MultiModal Intelligent Traffic Signal System (MMITSS) and V2X Hub are common examples of external operations.</p>
Summary of Operations	<p>Definition: Outside the knowledge of the controller. This implies external manipulation of the actual phase timing and/or interval timing – which is not related to the internal timing algorithms of the traffic controller. These inputs may determine the specific phase timing or the termination of a phase rather than the internal traffic control logic/timers.</p> <p>Examples of such external control “operations” might include the following:</p> <ul style="list-style-type: none"> • NEMA Control Commands <ul style="list-style-type: none"> ○ Older ATMS supervisory control used the NEMA inputs such as HOLD, FORCE-OFF, (PHASE/PEDESTRIAN) OMIT. Central systems transmit these “commands” to the traffic controller which changes state based on
	<pre> 5.2.5 Phase Control Table ... 5.2.5.4 Phase Hold Control phaseControlGroupHold OBJECT-TYPE SYNTAX INTEGER (0..255) ACCESS read-write STATUS mandatory DESCRIPTION "<Definition> This object is used to allow a remote entity to hold phases in the device. When a bit = 1, the device shall activate the System Phase Hold control for that phase. When a bit = 0, the device shall not activate the System Phase Hold control for that phase. Bit 7: Phase # = (phaseControlGroupNumber * 8) Bit 6: Phase # = (phaseControlGroupNumber * 8) - 1 Bit 5: Phase # = (phaseControlGroupNumber * 8) - 2 Bit 4: Phase # = (phaseControlGroupNumber * 8) - 3 Bit 3: Phase # = (phaseControlGroupNumber * 8) - 4 Bit 2: Phase # = (phaseControlGroupNumber * 8) - 5 Bit 1: Phase # = (phaseControlGroupNumber * 8) - 6 Bit 0: Phase # = (phaseControlGroupNumber * 8) - 7 The device shall reset this object to ZERO when in BACKUP Mode. A write to this object shall reset the Backup timer to ZERO (see unitBackupTime). <Object Identifier> 1.3.6.1.4.1.1.1206.4.2.1.1.5.1.4" REFERENCE "NEMA TS 2 Clause 3.5.3.11.1" ::= { phaseControlGroupEntry 4 } </pre>
	<p>receipt of the command – i.e., it terminates a phase (FORCE-OFF) or skips a phase (OMIT). The excerpt below is from NTCIP 1202:</p> <p>The controller should know that it is being remotely managed and could convey this information, but it affects the time remaining in a green; a FORCE-OFF will terminate the current green and start the clearance process (amber and all-red) and then start the next phase with calls for service. It should be noted that a FORCE-OFF is not required to terminate the phase; the phase could time-out before the FORCE-OFF is received depending on demand. This is supervisory control.</p> <p>Examples of the commands supported are listed in NTCIP 1202:</p>

```

PhaseControlGroupEntry ::= SEQUENCE {
  phaseControlGroupNumber    INTEGER,
  phaseControlGroupPhaseOmit INTEGER,
  phaseControlGroupPedOmit  INTEGER,
  phaseControlGroupHold     INTEGER,
  phaseControlGroupForceOff INTEGER,
  phaseControlGroupVehCall  INTEGER,
  phaseControlGroupPedCall  INTEGER }

```



Those highlighted are actual controls – where the “calls” are simply placing a request on the phase.

- These same functions (e.g., HOLD, FORCE-OFF, PHASE/PEDESTRIAN OMIT) can also be activated using the cabinet wiring – and can be applied by such devices as local preemptors, local TSP management devices. Historically, many “customized” operations were handled using these external signals.
- “Local” pushbutton operation (police control), and time of day, or local operator implementation of cabinet flash. (Signals on-off and flashing.)

For the controls indicated above, the traffic controller is unlikely to have any indication of what is about to occur until the command is received or the input is activated.

COMMENT: It may be necessary to require some changes to the traffic control cabinet wiring or hardware to provide SPaT and MAP information. As others have noted, it is likely that anything less than an ATC (or equivalent) with modified software and/or hardware upgrades will be required to join the CV ECO system.

Comment: Either the controller or the RSU need to be made aware such conditions so that it can manage the “confidence” of the data being provided to the RSU.

Notes:

- If the central computer system issues supervisory control over the local controller through the NTCIP input signals (e.g., HOLD, FORCE-OFF, OMIT) there are other input/settings which may affect the operation of the controller.
- HOLD essentially “freezes” the traffic controller in its current state— phase hold—and the controller will stay in that display until the HOLD line is released; then if there are calls on successive phases, it will service those calls. However, without other calls, the fully actuated controller may simply remain in the phase until there is another call – or until the HOLD is reapplied.

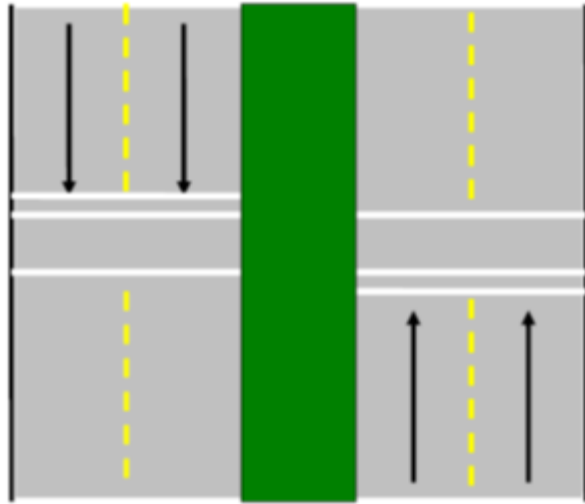
Source: Robert Rausch, TransCore.

2.6.2.6 High-Intensity Activated Crosswalk Beacon (HAWK)

Title	High-Intensity Activated Crosswalk Beacon (HAWK)
Summary of Operations	<p>A HAWK signal uses traditional traffic signal and pedestrian signal indications at crosswalks not located at the intersection of two roadways to assist pedestrian crossing a roadway. When not activated, the vehicle signal indications are blanked out (dark) and the crossing pedestrian signal indications display a steady “DON'T WALK.” The HAWK becomes active when a pedestrian call is placed to the controller (either through a pedestrian pushbutton or a direct input from a pedestrian sensor). Upon receiving a call, the following takes place:</p> <ul style="list-style-type: none"> • The vehicle signals start flashing yellow for a user programmed interval • After timing the activation interval, the vehicle signals transition to a solid yellow for specified interval, advising motorists to prepare to stop • After completing the transition interval, the vehicle traffic signals display a solid red. An optional “all-red” clearance interval is permitted. • After the optional clearance interval has expired, the pedestrian signal indication will display a solid “WALK” indication for a specified interval

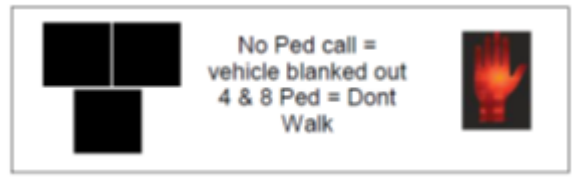
- After the "WALK" signal expires, the overhead vehicle signal displays an alternating flashing red signal to indicate that motorists may proceed when safe (after coming to a full stop). Simultaneously, the pedestrian is shown a flashing "DON'T WALK" with a countdown indicating the time left to cross.
- Once the pedestrian clearance interval has expired, the vehicle signal will transition to dark and the pedestrian indication will display a steady "DON'T WALK" indication. The intersection will rest in this state until activated by another pedestrian. Phase 4 and Phase 8 are phases for frontage road movements similar to through movements on a cross street.

Graphics

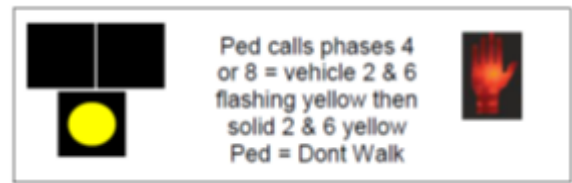


Typical Hawk Intersection diagram

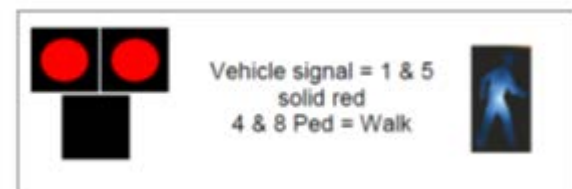
Initial State



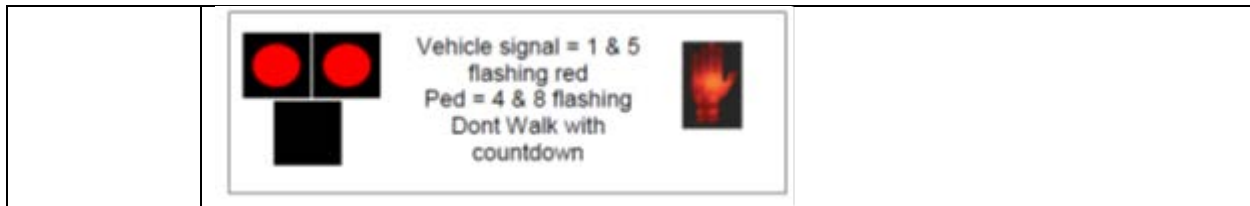
Activation and Vehicle Clearance



Pedestrian Interval



Pedestrian Clearance



Source: Kevin Balke, Texas A&M Transportation Institute.

2.6.2.7 Dynamic Lane Use

Title	Dynamic Lane Use
Summary of Operations	<p>Issue: Infrastructure owners goals include maximizing available capacity and reducing delay for all users of the built environment. As such, infrastructure owners are continuously exploring opportunities to respond to user demand for finite capacity. For signalized intersections, infrastructure owners may consider options to dynamically adjust allowable lane movements by time of day to meet an operational objective.</p> <p>Example 1: One common practice includes reversible lanes, or flex lanes, where a center lane is used for one-way operation entering an urban area during morning peak periods, and a reverse one-way operation is allowed to exit the urban area in an evening peak period. At signalized intersections, allowable left turn movements will change to avoid conflicts, and often use blank out signs (lane control signals) to indicate to drivers the allowable movement. Signal heads may go dark for off peak direction where use is prohibited.</p> <p>Example 2: A more recent variation is the dynamic left turn intersection introduced in 2020 in North Carolina. In this configuration, the number of allowable left-turn lane movements vary by time of day operation. During peak periods when left-turn demand is highest, dual left turn lanes are allowable as protected movements with signal heads displayed as green arrows as usual. In off-peak periods when left-turn demand is lower, only the inner (leftmost) left turn lane is an allowable movement that can be served as a permissive movement (e.g., flashing yellow arrow) or a protected one lane left turn movement to clear queued vehicles in the left turn lane. This allows mainline movement to be served more efficiently and reduce delay. Blank out signs may be used to inform drivers of allowable lane use.</p>
Graphics	<p>Reversible (flex lane) lane signal head transition at Route 173 (5400 S) and 2700 W in Taylorsville, Utah: Video: https://www.youtube.com/watch?v=xs1iix82hc4</p> <p>Dynamic Left Turn Intersection at Tyron Road and Cary Parkway in Cary, North Carolina, US70 Business at Town Center Boulevard in Clayton, North Carolina: Graphic: https://www.ncdot.gov/news/press-releases/Documents/Dynamic%20left%20turn%20graphic%20higher%20res.pdf Video: https://www.youtube.com/watch?v=Km-cz8rkLK4&feature=youtu.be</p>

Source: Matt D'Angelo, Gresham Smith.

2.7 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 this CI Implementation Guide. Three service packages in the ITS National Architecture fall into scope: TM04 Connected Vehicle Traffic Signal System, VS12 Pedestrian and Cyclist Safety, and SU05 Location and Time. Figure 8 shows the key interfaces from these three service packages and the flow of information that is exchanged among the Physical Objects that are within the scope of this CI Implementation Guide. Refer to Figure 2 to identify which of

these interfaces are addressed by the CI Implementation Guide. A Physical Object is a system or device that provides ITS functionality as part of ITS.

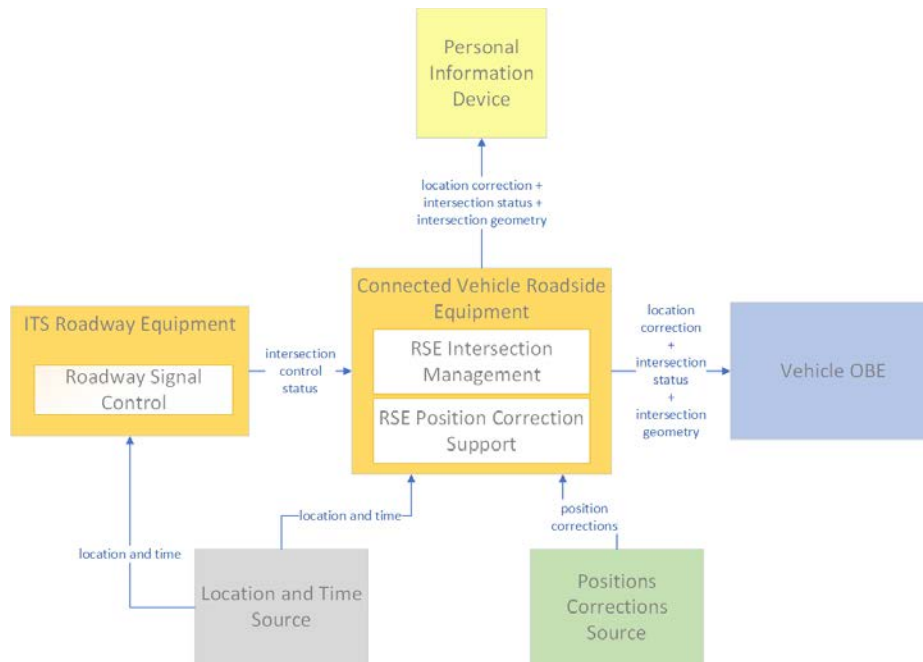


Figure 8. ARC-IT Physical View.

The Physical View of ARC-IT also defines the functions in each Physical Object, which are called Functional Objects (FO). The FOs that provide the functionality from the three service packages are described below.

- **Roadway Signal Control.** This FO includes the field elements that monitor and control signalized intersections. It includes the traffic signal controllers, detectors, conflict monitors, signal heads, and other ancillary equipment that supports traffic signal control. It also includes field masters and equipment that supports communications with a central monitoring and/or control system, as applicable. The communications link supports upload and download of signal timings and other parameters and reporting of current intersection status. It represents the field equipment used in all levels of traffic signal control from basic actuated systems that operate on fixed timing plans through adaptive systems. It also supports all signalized intersection configurations, including those that accommodate pedestrians.
- **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 traffic signal controller) to enhance traffic signal operations.
- **RSE Position Correction Support.** This FO broadcasts differential positioning data to enable precise locations to be determined by passing vehicles, supporting CV applications that require highly accurate positioning.

2.8 Testing and Conformity Verification Management

This section contains a framework for the testing that must be provided to verify that an implementation conforms to the CI Implementation Guide. This framework can be used to create a Verification Plan for the CI Implementation Guide, which will be described in more detail in later sections. Test Framework elements are described in the sections below.

2.8.1 Testing and Conformance

This section identifies needs to support testing that an implementation conforms to the CI Implementation Guide.

2.8.1.1 Conformance Statement

The CI test methodology needs to verify that a CI conforms with the CI Implementation Guide.

2.8.1.2 Conformance Definitions [Informative]

This section identifies terms relevant to conformance needs for a connected intersection.

2.8.1.2.1 Conformance

Conformance is how well something, such as a product, service or a system, meets the CI Implementation Guide.

2.8.1.2.2 Conformance Testing

Conformance testing is testing to determine whether a product or system meets the CI Implementation Guide.

2.8.1.2.3 Interface

The *IEEE Std 610.12-1990™, IEEE Standard Glossary of Software Engineering Terminology*, defines an interface as a shared boundary across which information is passed [*IEEE Std 610.12-1990*, p. 41].

The specification of this boundary, the system interface, is the focus of testing in this CI Implementation Guide. Testing of a system only through stimulus and response via interfaces is generally referred to as "Black box testing."

2.8.1.2.4 Interoperability

Interoperability is defined as the ability of two or more systems or components to exchange information and to use the information that has been exchanged [*IEEE Std 610.12-1990*, p. 42].

The purpose of interface testing as described in this CI Implementation Guide is to achieve interoperability between a CI and an OBU, and between a CI and a MU.

2.8.1.2.5 Interchangeability

Interchangeability reflects the capability to exchange devices of the same type on the same communications channel and have those devices interact with others devices of the same type using standards-based functions [*NTCIP Guide*, p. 2].

This definition is provided for discussion purposes as hardware interchangeability is out-of-scope, as described in Section 2.8.1.3.3, Clarifying Assumptions.

2.8.1.3 Testing and Conformance Scope Overview [Informative]

2.8.1.3.1 Testing and Conformance Scope Diagram

Figure 9 below, based on Figure 2. Connected Intersection, identifies the scoping elements for testing and conformance covered in this Implementation Guide.

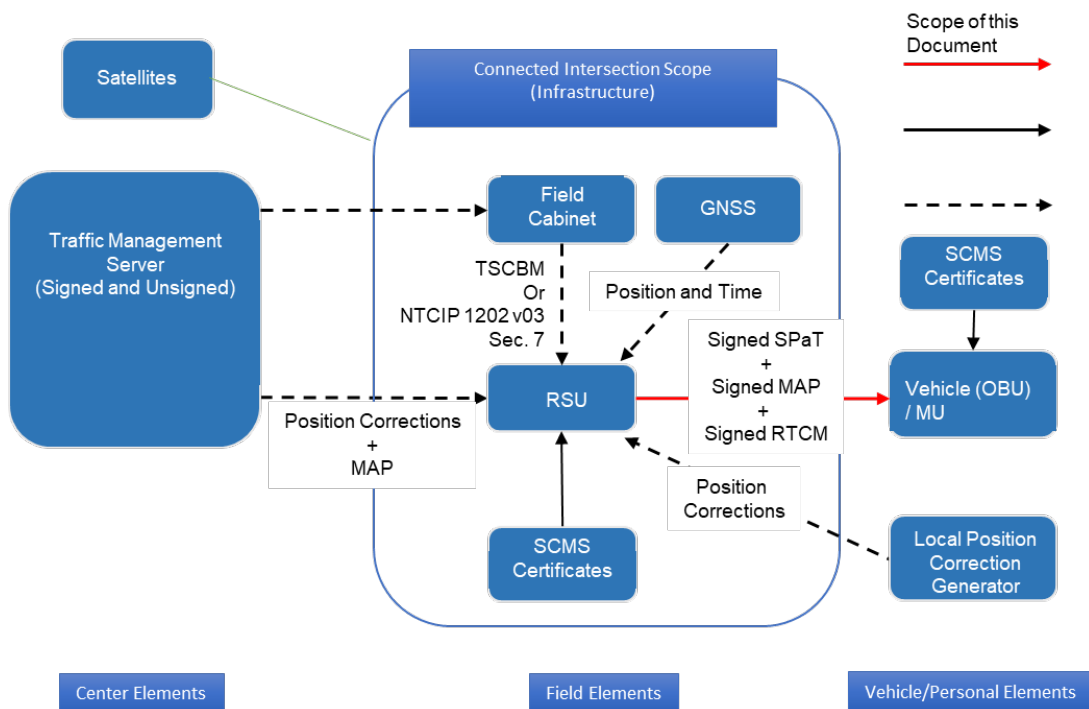


Figure 9. Testing and Conformity Scope Context Diagram.

- The dotted lines denote interface to the field equipment. Testing of these interfaces are outside the scope of this document.
- The solid arrow indicates supporting interface between the field equipment (RSU) and the SCMS system for security certificate. It is assumed that the RSU gets the valid certificates to digitally sign messages for transmission. Testing and verification of valid certificates is outside the scope of this document.
- The red arrow denotes the interface between digitally signed over-the-air SPaT, MAP, and RTCM message broadcast equipment (RSU) and the receiving device OBU/MU. Testing of this interface is within the scope of this document.

2.8.1.3.2 Testing and Conformance Scope Matrix

Table 1 below provides additional supporting detail related to testing and conformance scope.

Table 1. Testing and Conformance Scope Matrix

Scope Item	In-Scope (Yes/No/Limitations)
Device Interfaces (OBU, RSU, & Field Cabinet)	
Conformance	Yes (Limited to Messages / Data)
Minimum Performance	RSU (Limited to Broadcast Only)
Interoperability	Yes (Messages/Data Elements)
Hardware Interchangeability	As per <i>RSU Standard v1.0</i>
GNSS/GPS Accuracy (Position, Clock)	No
GNSS/GPS Elements	Yes (RTCM Messages/Data Elements)
RF & GNSS Interference	No
External Interfaces & Applications	
MAP Generation & its Realtime Accuracy	No
MAP Elements & its Usage Conformance	Yes (Messages/Data Elements)
MAP Security Profile	Yes (Digitally Signed Messages)

Scope Item	In-Scope (Yes/No/Limitations)
SPaT Generation & its Realtime Accuracy	Yes (Limited to Comparison of Packet Data Captured)
SPaT Elements & its Usage Conformance	Yes (Messages/Data Elements)
SPaT Security Profile	Yes (Digitally Signed Messages)
RTCM Generation & its Realtime Accuracy	No
RTCM Elements & its Usage Conformance	Yes (Messages/Data Elements)
RLVW Application Conformance	Yes (Messages/Data Elements)
RLVW Application Security	Yes (Digitally Signed Messages)
RLVW Application Interoperability	Yes (Limited / Broadcast Only)
RLVW Application Performance	No
SCMS Enrollment Process	No
SCMS Certificate Access	Yes
SCMS Device Loading	No
SCMS Transition (between expired and new certificates)	No
Traffic Management Server	No
Transportation Field Cabinet / equipment	No
Other Interfaces	
NTCIP 1202	No
NTCIP 1218	No

2.8.1.3.3 Clarifying Assumptions

- Testing the security system is out of scope for this CI Implementation Guide. However, testing will be with SCMS security in place.
- The SPaT information message will be an output via an interface from a device in the Transportation Field Cabinet to the RSU and that is a test point. The second test point is the SPaT message output from the RSU.
- The source of the MAP data is from a Map Data Server and may be exchanged with a device in the Transportation Field Cabinet or the Traffic Management System. The MAP data (possibly in the form of a MAP message) is then sent to the RSU and broadcast.
- The High Precision Positioning/Timing Source (HPP/TS) is typically contained within an RSU. However, the GNSS signal comes from the external environment (e.g., satellite).
- The RSU is capable of broadcasting Immediate Forwarding messages and Store and Repeat messages, as defined in NTCIP 1218.
- The TMS interacts directly with the RSU and/or through the Transportation Field Cabinet.
- Pedestrians activate crosswalks manually at intersections.

2.8.1.3.4 Testing and Conformance Objectives: Operational Verification and Conformance

- **SPaT/MAP.** Verify SPaT / MAP broadcast through over-the-air capture of data. While verification at the OBU/MU is outside the scope of this CI Implementation Guide, a data sniffer may be used as an alternative.
- **High Precision Positioning/Timing Source.** Verify Time and Location data provided from Satellites (Live) or from a Network at the RSU.
- **RSU.** Verify that the RSU transmits SPaT / MAP / RTCM messages. Receiver locations are unknown. Verification is achieved by over-the-air captures (i.e., verification of the captured data).
- **Vehicle (OBU).** Verify an OBU receives SPaT / MAP / RTCM Messages. While verification from the OBU is outside the scope of this CI Implementation Guide, a data sniffer may be used as an alternative.
- **Pedestrians (MU).** While verification from the MU is outside the scope of this CI Implementation Guide, a data sniffer may be used as an alternative.

2.8.1.4 Infrastructure Testing

The CI test methodology needs test procedures to ensure that the infrastructure provides data to the OBUs/MUs that conforms to the CI Implementation Guide.

2.8.1.4.1 Validate Message Data Needs

The CI test methodology needs to test/verify that a CI provides message data to the OBU/MU that conforms to the CI Implementation Guide. The message data needs are documented in Section 2.4.2, Traffic Signal Controller Infrastructure Data.

2.8.1.4.2 Reference Integrity Message Data Needs

The CI test methodology needs to test/verify referential integrity of CI message data that conforms to the CI Implementation Guide. For example, the intersection identifier for an intersection contained as part of the Signal Timing (SPaT) data must match the intersection identifier contained in a Road Geometry (MAP) for the intersection. Note: This may be a gap in the data content.

2.8.1.4.3 Verify Performance Needs

The CI test methodology needs test procedures to verify that the minimum performance criteria from the RSU to the OBU/MU to support in-vehicle basic RLVW application are fulfilled. The performance criteria includes data accuracy within defined tolerances, allowable latency, and periodicity.

2.8.2 Test Methodology

The CI test methodology needs to describe the methods and approach to testing.

2.8.2.1 Test Methodology Concepts [Informative]

Figure 10 illustrates a high-level concept for test execution and is an illustration of the contents presented in Table 1.

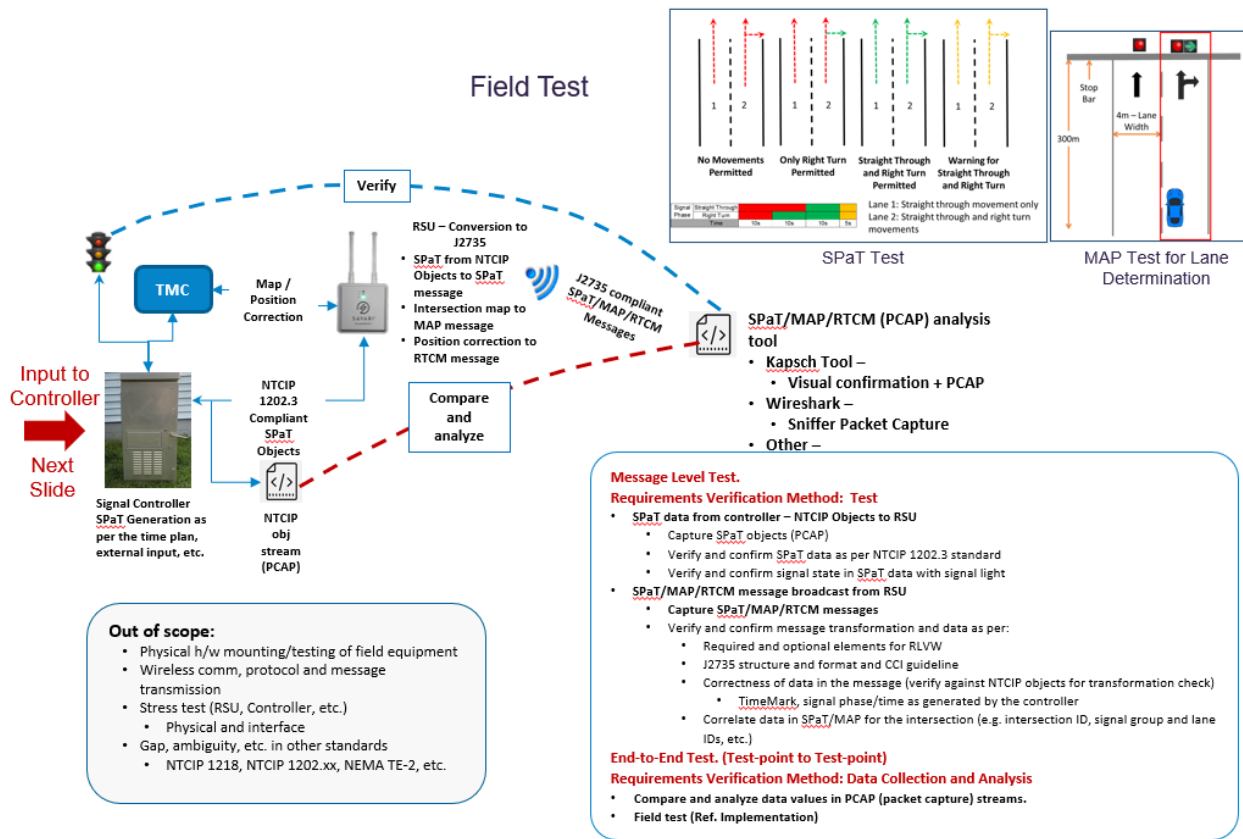


Figure 10. Test Methodology Concepts.

2.8.2.2 Test Environment

The CI test methodology needs to describe the test environment to provide a basis for comprehensive and consistent testing.

Figure 11 below provides additional detail regarding test environment elements related to SPaT testing.

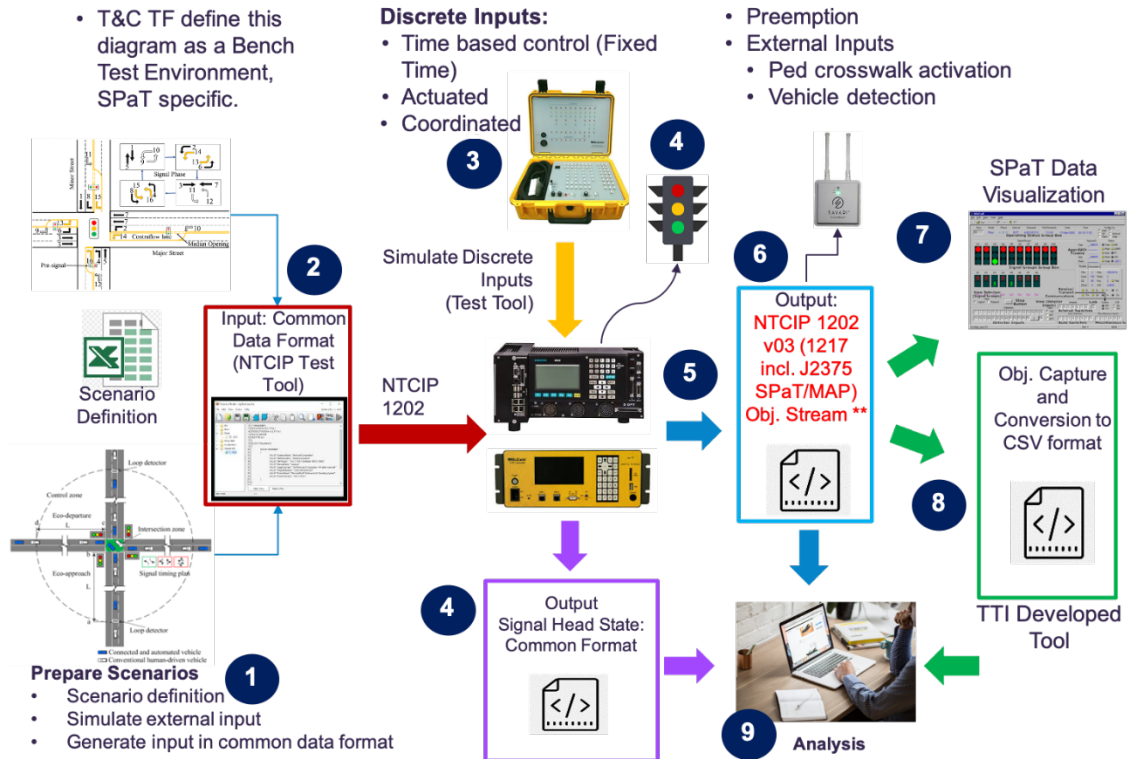


Figure 11. Example Test Environment for SPaT Testing.

The numbers reflect potential steps to be described in a test procedure. A high-level example is shown below.

1. Prepare operational test scenarios.
2. NTCIP Test tool test input (operational scenario) to Controller (e.g., from laptop).
3. Test tool (e.g., suitcase tester) generates discrete inputs to Controller. e.g., pedestrian crosswalk activation, vehicle detection
4. Controller output to Signal Head and to a file (CSV format).
5. Simultaneous with Step 4, Controller outputs NTCIP 1202 v03A (SPaT information message) for RSU.
6. Controller outputs from Step 5 are captured in a PCAP File.
7. Simultaneous with Step 6, a Visualization Tool shows Signal State and Controller Output destined for RSU.
8. Test tool (e.g., TTI Test Tool) converts byte-oriented SPaT information message or NTCIP 1202 v03A packets to a CSV file.
9. The output data captures from Controller are time synchronized to verify controller outputs are correct for a given set of initial inputs defined in steps 1, 2, and 3.

2.8.3 Message Level Testing

The CI test methodology needs to describe methods to test/verify the data format, data structure, and values of data content in messages.

2.8.3.1 Positive Testing

The CI test methodology needs to describe methods to test/verify positive outcomes/results when correct inputs are provided to the CI.

2.8.3.2 Negative Testing

The CI test methodology needs to describe methods to test/verify correct error handling when negative (incorrect) inputs are provided to the CI.

2.8.3.3 Boundary Testing

The CI test methodology needs to describe methods to test/verify correct error handling for boundary conditions (values) inputs are provided to the CI.

2.8.3.4 Packet Capture Analysis-based Testing

The CI test methodology needs to describe methods of data collection for analysis-based testing.

2.8.3.5 Field Environment Analysis

The CI test methodology needs to describe methods of data collection for analysis in field environments. For example, the SPaT matches the signal indication, and that the MAP represents the proper lane geometrics for lane determination.

2.8.4 Test Documentation

The CI test methodology needs to develop test documentation to guide comprehensive testing.

Test documentation, as described in *IEEE Std 829-2008 IEEE Standard for Software and System Test Documentation*, include the following:

- **Test Planning.**
 - **Test Plan.** Provides the requirements to be tested, test environment, staffing needs, agency resources, schedule, and test tools.
- **Requirements Verification.**
 - **Test Cases.** Provides the inputs to and outputs from the software or software-based system being tested to verify a requirement.
 - **Test Procedures.** Provide test steps required to execute each test case.
- **Test Execution.**
 - **Test Logs.** Provides a chronological record of relevant details about the execution of tests.
 - **Test Anomaly Reports.** Provides documentation of any event that occurs during the testing process that requires investigation.
- **Conformance Summary.**
 - **Test Summary Report.** Provides a summary of major testing activities, events, and results of testing, identifies anomalies and resolution status (resolved/unresolved), and relevant metrics collected.

Figure 12 below illustrates the relationships of the various test documentation described above.

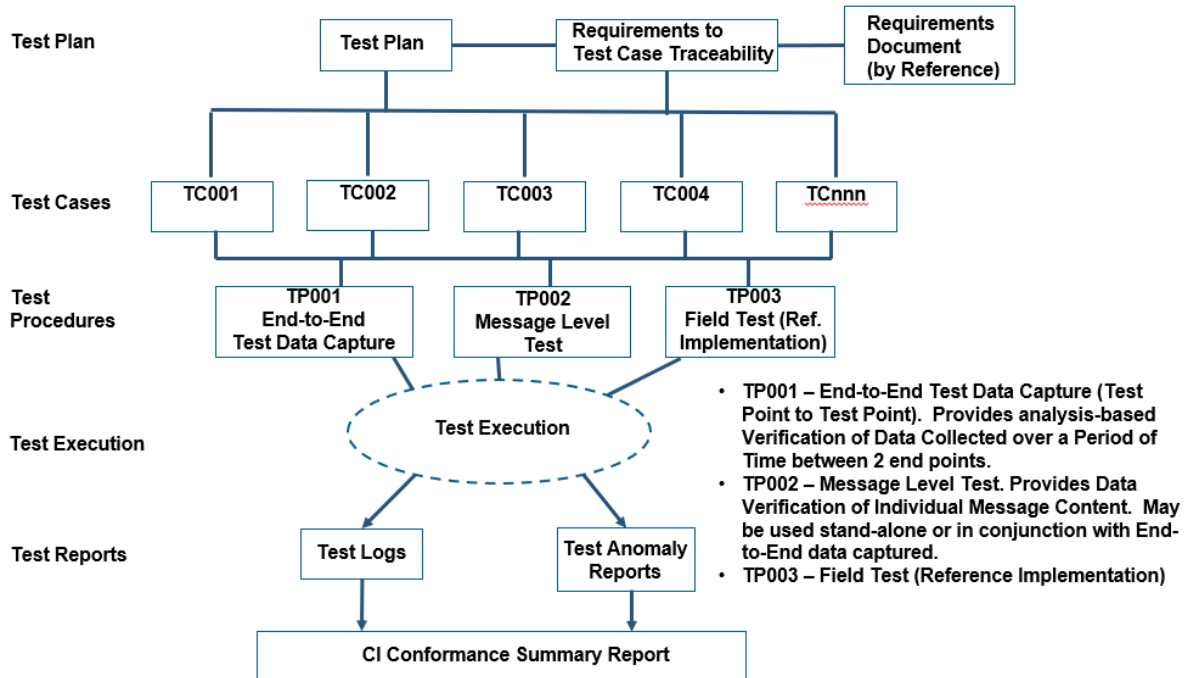


Figure 12. Test Documentation Relationships.

2.8.5 Requirements Verification Methods

The CI test methodology needs to describe the methods of requirements verification. It is generally accepted that there are the following four methods of requirements verification:

- **Inspection.** Examination of the system using one of your five senses. This test method is used for verification through a visual comparison that the requirement has been satisfied. For example, the Vendor shall provide training on the troubleshooting of the system, including local intersection and central portions.
- **Demonstration.** Manipulation of the system to verify that the results are as planned or expected. This test method is used for a requirement that the system can demonstrate without external test equipment.
- **Analysis.** Verification of system using models, calculations, and testing equipment. This test method is used for a requirement that is fulfilled indirectly through a logical conclusion or mathematical analysis of a result. For example, algorithms for congestion: the designer may need to show that the requirement is met through the analysis of count and occupancy calculations in software or firmware.
- **Test.** Verification of system using a controlled and predefined series of inputs to ensure specific and predefined outputs are produced. This test method is used for a requirement that requires some external piece of test equipment (such as logic analyzer or voltmeter).

2.8.6 Test Cases

The CI test methodology needs to describe test cases that define the test inputs and expected outcomes to verify one or more requirements.

2.8.7 Test Coverage

The CI test methodology needs to verify that testing provides coverage of all stated requirements.

NOTE: This may be done by verifying that test cases are developed for each requirement, at least once. Typically, a requirements to test case traceability matrix is used to assist with test coverage assessment.

2.8.8 Test Procedures

The CI test methodology needs a consistent set of procedures for executing test cases.

2.8.9 Identify Existing Test Documentation

The CI test methodology needs to gather information regarding available test documentation applicable to testing of connected intersections.

2.8.10 Configuration and Change Management Needs

The CI test methodology needs to perform testing when changes are made to the CI. These changes may include the following:

- CI Configuration Changes: software, firmware, hardware changes
- Changes in Standards: SAE J2735 version (2009, 2016, 2020, 2022, 2023)
- Message element table: Mandatory Elements, Optionals made Mandatory
- Controller Parameters: e.g., Timing plans

Section 3

Functional Requirements [Normative]

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

- a) A tutorial
- b) Needs to Requirements Traceability Matrix (NRTM) – A Functional Requirement is a requirement of a given function and therefore is only required to be implemented if the associated functionality (e.g., user need) is selected through the use of the NRTM. The NRTM also indicates which of the items are mandatory, conditional, or optional. The NRTM can be used by procurement personnel to specify the desired features for a connected intersection or can be used by an implementation to document the features supported by their implementation.
- c) Requirements – These are requirements that collectively satisfy the user needs identified in Section 2.5. These requirements provide the details so that a requirement can be fulfilled and validated.

Section 3 is intended for all readers, including the following:

- a) Transportation Managers
- b) Transportation Operators
- c) Transportation Engineers
- d) System Integrators
- e) Device Manufacturers
- f) Application Developers

For the first four categories of readers, Section 3 is useful in understanding the details of the CI Implementation Guide. For these readers, Section 3.2.3 is particularly useful in preparing procurement specifications and assists in mapping the various rows of this table to the more detailed text contained within the other sections.

For the next two categories of readers, this section is useful to fully understand what is required for conformance to this CI Implementation Guide. Table 5 in Section 3.2.3 may be used to document the capabilities of their implementations.

For application developers, this section is useful to understand the data provided by a connected intersection and what the data represents.

3.1 Tutorial [Informative]

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

3.2 Needs to Requirements Traceability Matrix

The NRTM, provided in Section 3.2.3, maps the user needs defined in Section 2 to the requirements defined in Section 3. The NRTM can be used by the following:

- a) A user or specification writer to indicate which requirements are to be implemented in a project-specific implementation
- b) The device manufacturer and user, as a detailed indication of the capabilities of the implementation

- c) A user, as a basis for initially checking the potential interoperability with another implementation
- d) A tester, as a checklist to compare against a specification and provide basis for test planning

3.2.1 Notation [Informative]

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

3.2.1.1 Conformance Symbols

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

Table 2. Conformance Symbols

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

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

3.2.1.2 Conditional Status Notation

The predicate notations in Table 3 may be used.

Table 3. Conditional Status Notation

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

The <predicate>: notation means that the status following it applies only when the NRTM states that the feature or features identified by the predicate are supported. In the simplest case, <predicate> is the identifying tag of a single NRTM item. The <predicate> notation may precede a table or group of tables in a section or subsection. When the group predicate is true then the associated section shall be completed. The symbol <predicate> also may be a Boolean expression composed of several indices. "AND," "OR," and "NOT" shall be used to indicate the Boolean logical operations.

The predicates used in this standard map to the sections indicated in Table 4.

Table 4. Predicate Mapping

Predicate	Section
DSRC	3.3.1.1
PC5	3.3.1.2
TestPro	3.4.1.4
TSCBM	3.3.2.1.1.2

3.2.1.3 Support Column Symbols

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

Table 5. Support Column Entries

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

3.2.2 Instructions for Completing the NRTM [Informative]

In the 'Support' column, each response shall be selected either from the indicated set of responses (for example: Yes / No / NA), or it shall reference additional items that are to be attached (for example, list of traffic signal controllers to be supported by an implementation). If a conditional requirement is inapplicable, use the Not Applicable (NA) choice.

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

3.2.2.1 Conformance Definition

To claim "Conformance" to this implementation guide, the manufacturer shall minimally fulfill the mandatory requirements as identified in the NRTM (see Section 3.2.3).

NOTE: The reader and user of this implementation guide is advised that 'conformance' to the CI Implementation Guide should not be confused with 'compliance' to a specification. The CI Implementation Guide is as broad as possible to allow a very simple CI implementation to be 'conformant' to the CI Implementation Guide. An agency specification needs to identify the requirements of a particular project and needs to require the support of those requirements. A specification writer is advised to match the requirements of a project with the corresponding standardized requirements defined in the CI Implementation Guide to achieve interoperability. This means that functions and requirements defined as 'optional' in the CI Implementation Guide might need to be selected in a specification (in effect made 'mandatory' for the project-specific specification).

A conformant device may offer additional (optional) features, as long as they are conformant with the requirements of the CI Implementation Guide and the standards it references (e.g., *SAE J2735_202007*). For example, to claim conformance to additional features, an implementation shall conform to all of the mandatory and selected optional requirements that trace to the subject user needs in the NRTM, AND shall fulfill the requirement by using all of the dialogs and data elements traced to the subject requirement in the Requirements Traceability Matrix (RTM).

NOTE: Off-the-shelf interoperability and interchangeability can only be obtained through well-documented features broadly supported by the industry as a whole. Designing a system that uses features not defined in a standard or not typically deployed in combination with one another inhibits the goals of interoperability and interchangeability, especially if the documentation of these features is not available for distribution to system integrators. Standards allow the use of additional features to support innovation, which is constantly needed within the industry; but users should be aware of the risks involved with using such features.

3.2.3 NRTM

In addition to the Conformance column and the Support column which were discussed in Sections 3.2.1.1 and 3.2.1.3, the additional columns in the NRTM table are the User Need ID and User Need columns, FR ID and Functional Requirements columns, and the Additional Specifications column.

- a) **User Need ID** - the number assigned to the user need statement. The user needs are defined within Section 2 and the NRTM is based upon the user needs within that Section.
- b) **User Need** – a short descriptive title identifying the user need.
- c) **FR ID** – the number assigned to the functional requirement statement. The requirements are defined within Section 3 and the NRTM references the traces from user needs to these requirements.
- d) **Functional Requirement** – a short descriptive title identifying the functional requirement.
- e) **Additional Specifications** - identifies other requirements to satisfy, including user selectable range values. The "Additional Specifications" column may (and should) be used by a procurement specification to provide additional notes and requirements for the product to be procured or may be used by an implementer to provide any additional details about the implementation. In some cases, default text already exists in this field, which the user should complete to fully specify the equipment. However, additional text can be added to this field as needed to fully specify a feature.

Table 6. Needs to Requirements Traceability Matrix

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	User Need	FR ID	Functional Requirement	Conformance	Support	Additional Specifications
2.4	Needs					
2.4.1	Architectural Needs					
		3.3.1.1 (DSRC)	IEEE Std 802.11-2016 (DSRC)	O.1 (1..*)	Yes / No	
		3.3.1.1.1.1	User Priority Level – SPaT Message	DSRC:M	Yes / NA	
		3.3.1.1.1.2	User Priority Level – MAP Message	DSRC:M	Yes / NA	
		3.3.1.1.1.3	User Priority Level – RTCMcorrections Message	DSRC:M	Yes / NA	
		3.3.1.2 (PC5)	3GPP PC5 Mode 4 (Release 14 or 15 (C-V2X))	O.1 (1..*)	Yes / No	
		3.3.1.2.1.1	ProSe Per Packet Priority – SPaT Message	PC5:M	Yes / NA	
		3.3.1.2.1.2	ProSe Per Packet Priority – MAP Message	PC5:M	Yes / NA	
		3.3.1.2.1.3	ProSe Per Packet Priority – RTCMcorrections Message	PC5:M	Yes / NA	
		3.3.1.2.2	One Shot Transmission	PC5:M	Yes / NA	
2.4.2	Traffic Signal Controller Infrastructure Data					
2.4.2.1	Provide Signal Timing Data to an RSU					
		3.3.2.1.1.1	NTCIP 1202 v03A SPaT Information	O.2 (1)	Yes / No	
		3.3.2.1.1.2 (TSCBM)	TSCBM SPaT Information	O.2 (1)	Yes / No	Not recommended for new implementations
		3.3.2.1.1.3	SPaT Message	O.2 (1)	Yes / No	
		3.3.2.1.2	TSC Infrastructure SPaT Information Message Transmission Rate	M	Yes	
		3.3.2.1.3	TSC Infrastructure SPaT Information Message Transmission Failure Threshold	M	Yes	
		3.3.2.1.4	TSC Infrastructure SPaT Information Average Message Update Latency	M	Yes	
		3.3.2.1.5	TSC Infrastructure Processing Latency	M	Yes	
2.4.2.2	Provide Signal Timing Status to an RSU					
		3.3.2.2.1	TSC Infrastructure Manual Control Indication	M	Yes	
		3.3.2.2.2	TSC Infrastructure Stop Time Indication	M	Yes	
		3.3.2.2.3	TSC Infrastructure Cabinet Flash (Exception Flash) Indication	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	User Need	FR ID	Functional Requirement	Conformance	Support	Additional Specifications
		3.3.2.2.4	TSC Infrastructure Controller Flash (Operational Flash) Indication	M	Yes	
		3.3.2.2.5	TSC Infrastructure Preemption Operation Indication	M	Yes	
		3.3.2.2.6	TSC Infrastructure Priority Operation Indication	M	Yes	
		3.3.2.2.7	TSC Infrastructure Fixed Time Control Indication	M	Yes	
		3.3.2.2.8	TSC Infrastructure Non-Fixed Time Control	M	Yes	
2.4.2.3	RLVW Support			M	Yes	
		3.3.2.3.1	TSC Infrastructure Assured Green End Time (AGET)	M	Yes	
		3.3.2.3.2	TSC Infrastructure Assured Green Period (AGP)	M	Yes	
		3.3.2.3.3	TSC Infrastructure Minimum End Time With AGP	M	Yes	
2.4.2.4	Receive Approaching Vehicle Information from an RSU			M	Yes	
2.4.3	Messages					
2.4.3.1	Message Performance Needs					
2.4.3.1.1	Uniform			M	Yes	
		3.3.3.1.1.1	SPaT Message - SAE J2735	M	Yes	
		3.3.3.1.1.2	SPaT Message - Mandatory Data Elements	M	Yes	
		3.3.3.1.1.3	SPaT Message - CI Mandatory Data Elements	M	Yes	
		3.3.3.1.1.4	SPaT Message PSID	M	Yes	
		3.3.3.1.1.5	MAP Message - SAE J2735	M	Yes	
		3.3.3.1.1.6	MAP Message - Mandatory Data Elements	M	Yes	
		3.3.3.1.1.7	MAP Message - Required Data Elements	M	Yes	
		3.3.3.1.1.8	MAP Message PSID	M	Yes	
		3.3.3.1.1.9	RTCMcorrections Message - SAE J2735	M	Yes	
		3.3.3.1.1.10	RTCMcorrections Message - Mandatory Data Elements	M	Yes	
		3.3.3.1.1.11	RTCMcorrections Message - Required Data Elements	M	Yes	
		3.3.3.1.1.12	RTCMcorrections Message PSID	M	Yes	
2.4.3.1.2	Robustness			M	Yes	
		3.3.3.1.2.1	Broadcast SPaT Message	M	Yes	
		3.3.3.3.2	Unknown Current Movement State for a Signal Group	M	Yes	
		3.3.3.3.4.2	Unknown Next Movement State	M	Yes	
		3.3.3.3.5.2	Unknown Time Change Detail	M	Yes	
		3.3.3.3.5.5	Unknown Maximum End Time	M	Yes	
2.4.3.1.3	Concise Messages			M	Yes	
		3.3.3.1.3.1	Transport Message Size - WAVE	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	User Need	FR ID	Functional Requirement	Conformance	Support	Additional Specifications
		3.3.3.1.3.2.1	Nodes by Offsets	M	Yes	
		3.3.3.1.3.2.2.1	Computed Lane - Lane Identifier	M	Yes	
		3.3.3.1.3.2.2.2	Computed Lane - X-Offset	M	Yes	
		3.3.3.1.3.2.2.3	Computed Lane - Y-Offset	M	Yes	
		3.3.3.1.3.2.2.4	Computed Lane - Angle	O	Yes / No	
2.4.3.1.4	Advanced Notification			M	Yes	
		3.3.3.1.4.1	Data Coverage - Every Lane	M	Yes	
		3.3.3.1.4.2	Advanced Notification - Time	M	Yes	
2.4.3.1.5	Timeliness			M	Yes	
		3.3.3.1.5.1	SPaT Message - Broadcast Periodicity	M	Yes	
		3.3.3.1.5.2	SPaT Message - Broadcast Latency	M	Yes	
		3.3.3.1.5.3	MAP Message - Broadcast Periodicity	M	Yes	
2.4.3.1.6	Quality Assurance			M	Yes	
		3.3.3.1.6.1	Completeness - SPaT Message	M	Yes	
		3.3.3.1.6.2	Completeness - MAP Message	M	Yes	
		3.3.3.3.2.13	No MAP Available	M	Yes	
		3.3.3.3.8	SPaT Message - Accuracy	M	Yes	
		3.3.3.4.7	MAP Message - Accuracy	M	Yes	
2.4.3.2	Generic Message Data Needs					
2.4.3.2.1	Time Source			M	Yes	
		3.3.3.2.1	Time Accuracy	M	Yes	
2.4.3.2.2	Message Revision			M	Yes	
		3.3.3.2.2.1	SPaT Message - Revision Counter Increment	M	Yes	
		3.3.3.2.2.2	SPaT Message - Revision Counter Not Increment	M	Yes	
		3.3.3.2.2.3	MAP Message - Revision Counter Increment	M	Yes	
		3.3.3.2.2.4	MAP Message - Revision Counter Not Increment	M	Yes	
		3.3.3.2.2.5	MAP Message - Intersection Revision Counter Increment	M	Yes	
		3.3.3.2.2.6	MAP Message - Intersection Revision Counter Not Increment	M	Yes	
		3.3.3.2.2.7	RTCMcorrections Message - Sequence Number Increment	M	Yes	
		3.3.3.2.2.8	RTCMcorrections Message - Sequence Number Not Increment	M	Yes	
2.4.3.2.3	Timestamp			M	Yes	
		3.3.3.2.3.1	SPaT Message - Message Time Stamp	M	Yes	
		3.3.3.2.3.2	SPaT Message - Intersection Time Stamp	M	Yes	
2.4.3.3	Signal Timing Data Needs					

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	User Need	FR ID	Functional Requirement	Conformance	Support	Additional Specifications
2.4.3.3.1	Intersection Identification			M	Yes	
		3.3.3.3.1.1	Intersection Signal Timing Information	M	Yes	
		3.3.3.3.1.2	Road Regulator Identifier	M	Yes	
		3.3.3.3.1.3	Intersection Reference Identifier	M	Yes	
2.4.3.3.2	Intersection Status			M	Yes	
		3.3.3.1.2.1	Broadcast SPaT Message	M	Yes	
		3.3.3.3.2.1	Manual Control	M	Yes	
		3.3.3.3.2.2	Stop Time	M	Yes	
		3.3.3.3.2.3	Failure Flash	M	Yes	
		3.3.3.3.2.4	Preemption	M	Yes	
		3.3.3.3.2.5	Priority	M	Yes	
		3.3.3.3.2.6	Fixed Time	M	Yes	
		3.3.3.3.2.7	Traffic Dependent Mode	M	Yes	
		3.3.3.3.2.8	Standby Mode	M	Yes	
		3.3.3.3.2.9	Failure Mode	M	Yes	
		3.3.3.3.2.10	Controller Off	M	Yes	
		3.3.3.3.2.11	Recent MAP Update	M	Yes	
		3.3.3.3.2.12	New Lane IDs	M	Yes	
		3.3.3.3.2.13	No MAP Available	M	Yes	
		3.3.3.3.2.14	No SPaT Available	M	Yes	
2.4.3.3.3	Current Movement State			M	Yes	
		3.3.3.3.3.1	Current Movement State for a Signal Group	M	Yes	
		3.3.3.3.3.2	Unknown Current Movement State for a Signal Group	M	Yes	
		3.3.3.3.3.3	Flashing Yellow Arrow Permissive Movement	M	Yes	
		3.3.3.3.3.4	Protected and Permissive Clearance	M	Yes	
		3.3.3.3.3.5	Resolve Protected Versus Permissive Movement	M	Yes	
		3.3.3.3.3.6	Conflict Causes Permissive	M	Yes	
		3.3.3.3.3.7	No Conflict Causes Protected	M	Yes	
		3.3.3.3.3.8	WALK State Enumeration (No Conflict)	M	Yes	
		3.3.3.3.3.9	WALK State Enumeration (Potential Conflict)	M	Yes	
		3.3.3.3.3.10	Flashing DON'T WALK State Enumeration	M	Yes	
		3.3.3.3.3.11	Steady DON'T WALK State Enumeration	M	Yes	
		3.3.3.3.3.12	Movement State for Signal Groups Identified	M	Yes	
2.4.3.3.4	Next Movement State			M	Yes	
		3.3.3.3.4.1	Next Movement State	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	User Need	FR ID	Functional Requirement	Conformance	Support	Additional Specifications
		3.3.3.3.4.2	Unknown Next Movement State	M	Yes	
		3.3.3.3.4.3	No Past State	M	Yes	
2.4.3.3.5	Time Change Details			M	Yes	
		3.3.3.3.5.1	Time Change Details	M	Yes	
		3.3.3.3.5.2	Unknown Time Change Detail	M	Yes	
		3.3.3.3.5.3	Minimum End Time	M	Yes	
		3.3.3.3.5.4	Maximum End Time	M	Yes	
		3.3.3.3.5.5	Unknown Maximum End Time	M	Yes	
		3.3.3.3.5.6	No Current Movement State Start Time	M	Yes	
		3.3.3.3.5.7	Next Movement State Start Time	M	Yes	
		3.3.3.3.5.8	Next State Start Time Equals Current State Minimum End Time	M	Yes	
2.4.3.3.6	Next Allowed Movement Time			M	Yes	
		3.3.3.3.6.1	Time of Next Allowed Movement	M	Yes	
2.4.3.3.7	Enabled Lanes			M	Yes	
		3.3.3.3.7	Enabled Lanes Indication	M	Yes	
2.4.3.3.8	Signal Timing and Roadway Indications Synchronization			M	Yes	
		3.3.3.1.5.2	SPaT Message - Broadcast Latency	M	Yes	
		3.3.3.3.8	SPaT Message - Accuracy	M	Yes	
2.4.3.4	Roadway Geometry Data Needs					
2.4.3.4.1	Intersection Geometry			M	Yes	
		3.3.3.4.1.1	Intersection Geometry Information	M	Yes	
		3.3.3.4.1.2	Intersection Geometry - Road Regulator Identifier	M	Yes	
		3.3.3.4.1.3	Intersection Geometry - Intersection Identifier	M	Yes	
		3.3.3.4.1.4.1	Intersection Reference Point - Position	M	Yes	
		3.3.3.4.1.4.2	Intersection Reference Point - Description	M	Yes	
		3.3.3.4.1.4.3	Intersection Reference Point Accuracy	M	Yes	
		3.3.3.4.1.5	Default Lane Width	M	Yes	
		3.3.3.4.1.6	Lane Identifier	M	Yes	
		3.3.3.4.1.7	Center of Vehicle Lane Geometry	M	Yes	
		3.3.3.4.1.8	Center of Crosswalk Lane Geometry	M	Yes	
		3.3.3.4.1.9	Center of Pedestrian Landings Geometry	M	Yes	
		3.3.3.4.1.10	Lane Description	M	Yes	
		3.3.3.4.1.11	First Node Point - Ingress Vehicle Lane	M	Yes	
		3.3.3.4.1.12	First Node Point - Egress Vehicle Lane	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	User Need	FR ID	Functional Requirement	Conformance	Support	Additional Specifications
		3.3.3.4.1.13	Node Offset from Intersection Reference Point	M	Yes	
		3.3.3.4.1.14	Node Elevation Offset from Intersection Reference Point	M	Yes	
		3.3.3.4.1.15	Offset from Previous Node	M	Yes	
		3.3.3.4.1.16	Elevation Offset from Previous Node	M	Yes	
		3.3.3.4.1.17	Advanced Notification - Ingress Vehicle Lane	M	Yes	
		3.3.3.4.1.18	End Nodes - Crosswalk Lane	M	Yes	
		3.3.3.4.1.19	End Nodes - Pedestrian Landing	M	Yes	
		3.3.3.4.1.20	Maximum Distance between Nodes	M	Yes	
		3.3.3.4.1.21	Maximum Number of Nodes	M	Yes	
		3.3.3.4.1.22	Node Lane Width	M	Yes	
		3.3.3.4.1.23	Node Accuracy	M	Yes	
2.4.3.4.2	Lane Attributes			M	Yes	
		3.3.3.4.2.1	Direction of Travel	M	Yes	
		3.3.3.4.2.2	Lane Sharing	M	Yes	
		3.3.3.4.2.3	Lane Type Attributes	M	Yes	
		3.3.3.4.2.4	Lane Attributes - Vehicle	M	Yes	
		3.3.3.4.2.5	Lane Attributes - Crosswalk	M	Yes	
		3.3.3.4.2.6	Lane Attributes - Bicycle	M	Yes	
		3.3.3.4.2.7	Lane Attributes - Tracked Vehicles	M	Yes	
		3.3.3.4.2.8	Lane Attributes - Parking	M	Yes	
2.4.3.4.3	Allowed Maneuvers			M	Yes	
		3.3.3.4.3	Lane Maneuvers	M	Yes	
2.4.3.4.4	Connections Between Lanes			M	Yes	
		3.3.3.4.4.1	Lane Connections	M	Yes	
		3.3.3.4.4.2	Connection Egress Lane	M	Yes	
		3.3.3.4.4.3	Connection Maneuvers	M	Yes	
		3.3.3.4.4.4	Connection Signal Group	M	Yes	
		3.3.3.4.4.5	Include Only Permitted Connections	M	Yes	
2.4.3.4.5	Approach Speed Limit Information			M	Yes	
		3.3.3.4.5.1	Default Speed Limit	M	Yes	
		3.3.3.4.5.2	Change in Lane Speed Limit	O	Yes / No	
2.4.3.4.6	Revocable Lanes			M	Yes	
		3.3.3.4.6	Revocable Lanes	M	Yes	
2.4.3.4.7	Road Geometry Accuracy			M	Yes	
		3.3.3.4.1.23	Node Accuracy	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	User Need	FR ID	Functional Requirement	Conformance	Support	Additional Specifications
		3.3.3.4.7	MAP Message - Accuracy	M	Yes	
2.4.3.4.8	Signal Timing and Roadway Geometry Synchronization			M	Yes	
		3.3.3.4.8.1	Matching Intersection Reference Identifier	M	Yes	
		3.3.3.4.8.2	Matching SPaT and MAP Version	M	Yes	
2.4.3.5	Positioning Data Needs					
2.4.3.5.1	Positioning Corrections Data Format			O	Yes / No	
		3.3.3.5.1	Positioning Corrections	M	Yes	
2.4.3.5.2	Real-Time Kinematic Corrections			M	Yes	
		3.3.3.5.2.1	RSU Proximity	M	Yes	
		3.3.3.5.2.2	Minimum RTCM Corrections Broadcast Frequency	M	Yes	
2.4.4	Security					
2.4.4.1	Correct Operations					
2.4.4.1.1	Operations - Data Trustworthiness			M	Yes	
		3.3.4.1.1	SPaT Information Message Trustworthiness - RSU	M	Yes	
		3.3.4.1.2	SPaT Information Message Trustworthiness - TSC Infrastructure	M	Yes	
		3.3.4.1.3	MAP Data Trustworthiness	M	Yes	
		3.3.4.1.4	RTCM Corrections Data Trustworthiness	M	Yes	
		3.3.4.2.1	Secure Network	M	Yes	
		3.3.4.2.2	Assurance of Connection to Correct Network	M	Yes	
		3.3.4.3.1	Security Compliance Assessment	M	Yes	
		3.3.4.3.2	Point of Certification	M	Yes	
		3.3.4.4.1	Certificate Issuance	M	Yes	
		3.3.4.4.2	Certificate Nonissuance	M	Yes	
		3.3.4.4.3	CI Operation Security Practices	M	Yes	
		3.3.4.4.4	RSU Security Standards	M	Yes	
		3.3.4.4.5	TSC Infrastructure Security Standards	M	Yes	
		3.3.4.6.1.2.1	(D)TLS Authentication - Installation	M	Yes	
		3.3.4.6.1.2.2	(D)TLS Authentication - Rejection	M	Yes	
		3.3.4.6.1.2.3	RSU Certificate Security	M	Yes	
		3.3.4.6.1.2.4	RSU Client Certificate Security	M	Yes	
		3.3.4.6.2	Interface between RSU and SCMS	M	Yes	
		3.3.4.6.3	Interface between an RSU and the OBU/MU	M	Yes	
		3.3.4.6.4.1	Use of Secure Transport Protocol	M	Yes	
		3.3.4.6.4.2	Use of TLS Protocol	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	User Need	FR ID	Functional Requirement	Conformance	Support	Additional Specifications
		3.3.4.6.4.4	Validation of Forwarded V2X Messages	M	Yes	
		3.3.4.6.5	Interface between the TMS and the TSC Infrastructure	M	Yes	
		3.3.4.6.6.1	Secure Connection to MAP Server	M	Yes	
		3.3.4.6.6.2	MAP Data Integrity	M	Yes	
		3.3.4.6.6.3	MAP Data Signature	M	Yes	
		3.3.4.6.7	Interface between MAP Server and the SCMS	M	Yes	
		3.3.4.7.3	RSU Device Class Requirement	M	Yes	
		3.3.4.7.4	TSC Device Class Requirement	M	Yes	
	3.3.4.7.5	MAP Signer Device Class Requirement	M	Yes		
2.4.4.1.2	Data Processing			M	Yes	
		3.3.4.1.2	SPaT Information Message Trustworthiness - TSC Infrastructure	M	Yes	
		3.3.4.4.3	CI Operation Security Practices	M	Yes	
		3.3.4.4.4	RSU Security Standards	M	Yes	
		3.3.4.4.5	TSC Infrastructure Security Standards	M	Yes	
		3.3.4.6.3	Interface between an RSU and the OBU/MU	M	Yes	
		3.3.4.7.3	RSU Device Class Requirement	M	Yes	
		3.3.4.7.4	TSC Device Class Requirement	M	Yes	
	3.3.4.7.5	MAP Signer Device Class Requirement	M	Yes		
2.4.4.1.3	Input Validation			M	Yes	
		3.3.4.4.3	CI Operation Security Practices	M	Yes	
		3.3.4.4.4	RSU Security Standards	M	Yes	
		3.3.4.4.5	TSC Infrastructure Security Standards	M	Yes	
		3.3.4.6.1.2.1	(D)TLS Authentication - Installation	M	Yes	
		3.3.4.6.1.2.2	(D)TLS Authentication - Rejection	M	Yes	
		3.3.4.6.2	Interface between RSU and SCMS	M	Yes	
		3.3.4.6.3	Interface between an RSU and the OBU/MU	M	Yes	
		3.3.4.7.3	RSU Device Class Requirement	M	Yes	
		3.3.4.7.4	TSC Device Class Requirement	M	Yes	
	3.3.4.7.5	MAP Signer Device Class Requirement	M	Yes		
2.4.4.1.4	Cyber Attacks			M	Yes	
		3.3.4.2.1	Secure Network	M	Yes	
		3.3.4.5.1	Cyber-Attack Recovery Plan	M	Yes	
		3.3.4.5.2	Cyber-Attack Robustness	M	Yes	
		3.3.4.5.3	Network Protection	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	User Need	FR ID	Functional Requirement	Conformance	Support	Additional Specifications
		3.3.4.6.1.2.1	(D)TLS Authentication - Installation	M	Yes	
		3.3.4.6.1.2.2	(D)TLS Authentication - Rejection	M	Yes	
		3.3.4.6.1.2.3	RSU Certificate Security	M	Yes	
		3.3.4.6.1.2.4	RSU Client Certificate Security	M	Yes	
		3.3.4.6.4.1	Use of Secure Transport Protocol	M	Yes	
		3.3.4.6.4.2	Use of TLS Protocol	M	Yes	
		3.3.4.6.4.3	Protection against TSC Infrastructure Reconfiguration from the RSU	M	Yes	
		3.3.4.6.5	Interface between the TMS and the TSC Infrastructure	M	Yes	
		3.3.4.7.1.1	RSU Protection	M	Yes	
		3.3.4.7.1.2	Device Protection	M	Yes	
		3.3.4.7.2.1	Secure RSU Administration User Interface	M	Yes	
		3.3.4.7.2.2	Password Change Prompt	M	Yes	
		3.3.4.7.3	RSU Device Class Requirement	M	Yes	
		3.3.4.7.4	TSC Device Class Requirement	M	Yes	
		3.3.4.7.5	MAP Signer Device Class Requirement	M	Yes	
2.4.4.1.5	Cyber Attacks Recovery			M	Yes	
		3.3.4.5.1	Cyber-Attack Recovery Plan	M	Yes	
		3.3.4.5.2	Cyber-Attack Robustness	M	Yes	
		3.3.4.6.2	Interface between RSU and SCMS	M	Yes	
		3.3.4.7.1.1	RSU Protection	M	Yes	
		3.3.4.7.1.2	Device Protection	M	Yes	
		3.3.4.7.2.3	Remote Restart	M	Yes	
		3.3.4.7.3	RSU Device Class Requirement	M	Yes	
		3.3.4.7.4	TSC Device Class Requirement	M	Yes	
3.3.4.7.5	MAP Signer Device Class Requirement	M	Yes			
2.4.4.1.6	Resilience			M	Yes	
		3.3.4.2.2	Assurance of Connection to Correct Network	M	Yes	
		3.3.4.5.1	Cyber-Attack Recovery Plan	M	Yes	
		3.3.4.7.1.1	RSU Protection	M	Yes	
		3.3.4.7.1.2	Device Protection	M	Yes	
		3.3.4.7.3	RSU Device Class Requirement	M	Yes	
		3.3.4.7.4	TSC Device Class Requirement	M	Yes	
3.3.4.7.5	MAP Signer Device Class Requirement	M	Yes			
2.4.4.1.7	Secure Administration			M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	User Need	FR ID	Functional Requirement	Conformance	Support	Additional Specifications
		3.3.4.7.2.1	Secure RSU Administration User Interface	M	Yes	
		3.3.4.7.2.2	Password Change Prompt	M	Yes	
		3.3.4.7.2.3	Remote Restart	M	Yes	
		3.3.4.7.2.4	Log Restarts	M	Yes	
		3.3.4.7.2.5	Factory Default	O	Yes / No	
		3.3.4.7.2.6	Protection against Tampering	M	Yes	
		3.3.4.7.2.7	Operational, Security and other Events Logging - RSU	M	Yes	
		3.3.4.7.2.8	Operational Logging - TMS	M	Yes	
		3.3.4.7.2.9	Operational Logging - TSC Infrastructure	M	Yes	
		3.3.4.7.2.10	Determine Mode of Operations	M	Yes	
		3.3.4.7.2.11	Determine Operational Status	M	Yes	
		3.3.4.7.2.12	Determine Operational Performance	M	Yes	
		3.3.4.7.2.13	Determine Operating Environment	M	Yes	
		3.3.4.7.2.14	Access Control Policy	M	Yes	
		3.3.4.7.3	RSU Device Class Requirement	M	Yes	
		3.3.4.7.4	TSC Device Class Requirement	M	Yes	
		3.3.4.7.5	MAP Signer Device Class Requirement	M	Yes	
		3.3.4.7.6.1	RSU Software and Firmware Updates	M	Yes	
		3.3.4.7.6.2	Trustworthiness of Software and Firmware Updates	M	Yes	
2.4.4.1.8	Authenticated Secure Update			M	Yes	
		3.3.4.7.2.5	Factory Default	M	Yes	
		3.3.4.7.3	RSU Device Class Requirement	M	Yes	
		3.3.4.7.4	TSC Device Class Requirement	M	Yes	
		3.3.4.7.5	MAP Signer Device Class Requirement	M	Yes	
		3.3.4.7.6.1	RSU Software and Firmware Updates	M	Yes	
		3.3.4.7.6.2	Trustworthiness of Software and Firmware Updates	M	Yes	
		3.3.4.7.6.3	TSC Infrastructure Software and Firmware Updates	M	Yes	
2.4.4.1.9	Assurance of Correct Network			M	Yes	
		3.3.4.2.2	Assurance of Connection to Correct Network	M	Yes	
		3.3.4.7.3	RSU Device Class Requirement	M	Yes	
		3.3.4.7.4	TSC Device Class Requirement	M	Yes	
		3.3.4.7.5	MAP Signer Device Class Requirement	M	Yes	
2.4.4.1.10	Secure Backend			M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	User Need	FR ID	Functional Requirement	Conformance	Support	Additional Specifications
2.4.4.1.11	Physical Security			M	Yes	
2.4.4.1.12	Device/System Monitoring			M	Yes	
2.4.4.2	Data Flow: Communications and Interface Security					
2.4.4.2.1	Data Flow Trustworthiness			M	Yes	
		3.3.4.6.1.1.1	Secure Transport of SNMPv3	M	Yes	
		3.3.4.6.1.1.2	Use of (D)TLS for Management Protocols	M	Yes	
		3.3.4.6.1.1.3	Use of SSH	M	Yes	
		3.3.4.6.1.2.1	(D)TLS Authentication - Installation	M	Yes	
		3.3.4.6.1.2.2	(D)TLS Authentication - Rejection	M	Yes	
		3.3.4.6.1.2.3	RSU Certificate Security	M	Yes	
		3.3.4.6.1.2.4	RSU Client Certificate Security	M	Yes	
		3.3.4.6.2	Interface between RSU and SCMS	M	Yes	
		3.3.4.6.3	Interface between an RSU and the OBU/MU	M	Yes	
		3.3.4.6.4.1	Use of Secure Transport Protocol	M	Yes	
		3.3.4.6.4.2	Use of TLS Protocol	M	Yes	
		3.3.4.6.4.4	Validation of Forwarded V2X Messages	M	Yes	
		3.3.4.6.5	Interface between the TMS and the TSC Infrastructure	M	Yes	
		3.3.4.6.6.1	Secure Connection to MAP Server	M	Yes	
		3.3.4.6.6.2	MAP Data Integrity	M	Yes	
		3.3.4.6.6.3	MAP Data Signature	M	Yes	
		3.3.4.6.7	Interface between MAP Server and the SCMS	M	Yes	
2.4.4.2.2	Data Integrity			M	Yes	
		3.3.4.6.1.1.1	Secure Transport of SNMPv3	M	Yes	
		3.3.4.6.1.1.2	Use of (D)TLS for Management Protocols	M	Yes	
		3.3.4.6.1.1.3	Use of SSH	M	Yes	
		3.3.4.6.3	Interface between an RSU and the OBU/MU	M	Yes	
		3.3.4.6.4.1	Use of Secure Transport Protocol	M	Yes	
		3.3.4.6.4.2	Use of TLS Protocol	M	Yes	
		3.3.4.6.5	Interface between the TMS and the TSC Infrastructure	M	Yes	
		3.3.4.6.6.1	Secure Connection to MAP Server	M	Yes	
		3.3.4.6.6.2	MAP Data Integrity	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	User Need	FR ID	Functional Requirement	Conformance	Support	Additional Specifications
		3.3.4.6.6.3	MAP Data Signature	M	Yes	
2.4.4.2.3	Data Confidentiality			M	Yes	
		3.3.4.6.1.1.1	Secure Transport of SNMPv3	M	Yes	
		3.3.4.6.1.1.2	Use of (D)TLS for Management Protocols	M	Yes	
		3.3.4.6.1.1.3	Use of SSH	M	Yes	
		3.3.4.6.6.1	Secure Connection to MAP Server	M	Yes	
2.4.4.3	Network Monitoring					
2.4.4.3.1	Misbehavior Reporting by Network Administrators			M	Yes	
		3.3.4.7.2.6	Protection against Tampering	M	Yes	
		3.3.4.7.2.7	Operational, Security and other Events Logging - RSU	M	Yes	
		3.3.4.8	Network Monitoring Requirements	M	Yes	
2.4.4.4	Credential Management			M	Yes	
2.4.4.4.1	Credential Provisioning			M	Yes	
		3.3.4.9.1.1	Start-up Initialization	M	Yes	
		3.3.4.9.1.2	Credential Updates	M	Yes	
2.4.4.4.2	Management of Untrustworthy Devices			M	Yes	
		3.3.4.9.2.1	Monitor Certificate Status	M	Yes	
		3.3.4.9.2.2	Drop Connections	M	Yes	
2.4.4.4.3	Credentialing System Access			M	Yes	
		3.3.4.6.2	Interface between RSU and SCMS	M	Yes	
		3.3.4.9.3.1	Connectivity Requirement	M	Yes	
		3.3.4.9.3.2	Download SCMS Files	M	Yes	
2.4.5	Operations and Maintenance Needs			M	Yes	
2.4.5.1	Interoperability			M	Yes	
2.4.5.2	Lifecycle			M	Yes	
2.4.5.3	Maintenance			M	Yes	
2.4.5.4	System Diagnostic Interface			M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	User Need	FR ID	Functional Requirement	Conformance	Support	Additional Specifications
2.4.5.5	System Performance Monitoring			M	Yes	
2.4.5.6	System Upgradeability			M	Yes	
2.8	Testing and Conformity Verification Management					
2.8.1	Testing and Conformance					
2.8.1.1	Conformance Statement			M	Yes	
	3.2.2.1	Conformance Definition		M	Yes	
2.8.1.2	Conformance Definitions [Informative]					
2.8.1.3	Testing and Conformance Scope Overview [Informative]					
2.8.1.4	Infrastructure Testing					
2.8.1.4.1	Validate Message Data Needs			O	Yes / No	
	3.4.1.2.1	Test Items		M	Yes	
	3.4.1.2.2	Features to be Tested		M	Yes	
	3.4.1.2.3	Features not to be Tested		M	Yes	
	3.4.1.2.4	Test Coverage		M	Yes	
	3.4.1.2.5	Item Pass/Fail Criteria		M	Yes	
	3.4.1.2.6	Requirements to Test Case Traceability Matrix		M	Yes	
	3.4.1.2.7	Organization Requirements		M	Yes	
	3.4.1.2.8	Roles and Responsibilities		M	Yes	
	3.4.1.2.9	Resources Summary		M	Yes	
	3.4.1.2.10	Test Schedule		M	Yes	
	3.4.1.2.11	Document Procedures and History		M	Yes	
2.8.1.4.2	Reference Integrity Message Data Needs			O	Yes / No	
	3.4.1.4.1	Test Procedure Identifier		M	Yes	
	3.4.1.4.2	Test Case References		M	Yes	
	3.4.1.4.3	Requirements Verification Method(s)		M	Yes	
	3.4.1.4.4	Procedure Descriptions		M	Yes	
	3.4.1.4.5	Procedure Steps		M	Yes	
	3.4.1.4.6	Relationship to other Procedures		M	Yes	
	3.4.1.4.7	Procedure Special Requirements		M	Yes	
2.8.2	Test Methodology					
2.8.2.1	Test Methodology Concepts [Informative]					

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	User Need	FR ID	Functional Requirement	Conformance	Support	Additional Specifications
2.8.2.2	Test Environment			O	Yes / No	
		3.4.1.2.1	Test Items	M	Yes	
		3.4.1.2.2	Features to be Tested	M	Yes	
		3.4.1.2.3	Features not to be Tested	M	Yes	
		3.4.1.2.4	Test Coverage	M	Yes	
		3.4.1.2.5	Item Pass/Fail Criteria	M	Yes	
		3.4.1.2.6	Requirements to Test Case Traceability Matrix	M	Yes	
		3.4.1.2.7	Organization Requirements	M	Yes	
		3.4.1.2.8	Roles and Responsibilities	M	Yes	
		3.4.1.2.9	Resources Summary	M	Yes	
		3.4.1.2.10	Test Schedule	M	Yes	
		3.4.1.2.11	Document Procedures and History	M	Yes	
2.8.3	Message Level Testing					
2.8.3.1	Positive Testing			M	Yes	
		3.4.1.4.1	Test Procedure Identifier	M	Yes	
		3.4.1.4.2	Test Case References	M	Yes	
		3.4.1.4.3	Requirements Verification Method(s)	M	Yes	
		3.4.1.4.4	Procedure Descriptions	M	Yes	
		3.4.1.4.4.1	Message Level Testing	M	Yes	
		3.4.1.4.4.1.1	Positive Testing	M	Yes	
		3.4.1.4.5	Procedure Steps	M	Yes	
		3.4.1.4.6	Relationship to other Procedures	M	Yes	
		3.4.1.4.7	Procedure Special Requirements	M	Yes	
2.8.3.2	Negative Testing			O	Yes / No	
		3.4.1.4.1	Test Procedure Identifier	M	Yes	
		3.4.1.4.2	Test Case References	M	Yes	
		3.4.1.4.3	Requirements Verification Method(s)	M	Yes	
		3.4.1.4.4	Procedure Descriptions	M	Yes	
		3.4.1.4.4.1	Message Level Testing	M	Yes	
		3.4.1.4.4.1.2	Negative Testing	M	Yes	
		3.4.1.4.5	Procedure Steps	M	Yes	
		3.4.1.4.6	Relationship to other Procedures	M	Yes	
		3.4.1.4.7	Procedure Special Requirements	M	Yes	
2.8.3.3	Boundary Testing			O	Yes / No	
		3.4.1.4.1	Test Procedure Identifier	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	User Need	FR ID	Functional Requirement	Conformance	Support	Additional Specifications
		3.4.1.4.2	Test Case References	M	Yes	
		3.4.1.4.3	Requirements Verification Method(s)	M	Yes	
		3.4.1.4.4	Procedure Descriptions	M	Yes	
		3.4.1.4.4.1	Message Level Testing	M	Yes	
		3.4.1.4.4.1.3	Boundary Testing	M	Yes	
		3.4.1.4.5	Procedure Steps	M	Yes	
		3.4.1.4.6	Relationship to other Procedures	M	Yes	
	3.4.1.4.7	Procedure Special Requirements	M	Yes		
2.8.3.4	Packet Capture Analysis-based Testing			O	Yes / No	
		3.4.1.4.1	Test Procedure Identifier	M	Yes	
		3.4.1.4.2	Test Case References	M	Yes	
		3.4.1.4.3	Requirements Verification Method(s)	M	Yes	
		3.4.1.4.4	Procedure Descriptions	M	Yes	
		3.4.1.4.4.2	End-to-End Testing - Packet Capture Analysis-based Testing	M	Yes	
		3.4.1.4.5	Procedure Steps	M	Yes	
		3.4.1.4.6	Relationship to other Procedures	M	Yes	
	3.4.1.4.7	Procedure Special Requirements	M	Yes		
2.8.3.5	Field Environment Analysis			O	Yes / No	
		3.4.1.4.1	Test Procedure Identifier	M	Yes	
		3.4.1.4.2	Test Case References	M	Yes	
		3.4.1.4.3	Requirements Verification Method(s)	M	Yes	
		3.4.1.4.4	Procedure Descriptions	M	Yes	
		3.4.1.4.4.3	Field Environment Testing	M	Yes	
		3.4.1.4.5	Procedure Steps	M	Yes	
		3.4.1.4.6	Relationship to other Procedures	M	Yes	
	3.4.1.4.7	Procedure Special Requirements	M	Yes		
2.8.4	Test Documentation			O	Yes / No	
		3.4.1.2.1	Test Items	M	Yes	
		3.4.1.2.2	Features to be Tested	M	Yes	
		3.4.1.2.3	Features not to be Tested	M	Yes	
		3.4.1.2.4	Test Coverage	M	Yes	
		3.4.1.2.5	Item Pass/Fail Criteria	M	Yes	
		3.4.1.2.6	Requirements to Test Case Traceability Matrix	M	Yes	
		3.4.1.2.7	Organization Requirements	M	Yes	
		3.4.1.2.8	Roles and Responsibilities	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	User Need	FR ID	Functional Requirement	Conformance	Support	Additional Specifications
		3.4.1.2.9	Resources Summary	M	Yes	
		3.4.1.2.10	Test Schedule	M	Yes	
		3.4.1.2.11	Document Procedures and History	M	Yes	
		3.4.1.3.1	Test Case Identifier	M	Yes	
		3.4.1.3.2	Inputs	M	Yes	
		3.4.1.3.3	Outcomes	M	Yes	
		3.4.1.3.4	Feature Pass/Fail Criteria	M	Yes	
		3.4.1.3.5	Intercase Dependencies	M	Yes	
		3.4.1.4 (TestPro)	Test Procedure Requirements	O	Yes / No	
		3.4.1.4.1	Test Procedure Identifier	TestPro:M	Yes / NA	
		3.4.1.4.2	Test Case References	TestPro:M	Yes / NA	
		3.4.1.4.3	Requirements Verification Method(s)	TestPro:M	Yes / NA	
		3.4.1.4.4	Procedure Descriptions	TestPro:M	Yes / NA	
		3.4.1.4.5	Procedure Steps	TestPro:M	Yes / NA	
		3.4.1.4.6	Relationship to other Procedures	TestPro:M	Yes / NA	
		3.4.1.4.7	Procedure Special Requirements	TestPro:M	Yes / NA	
		3.4.1.5.1	Test Log - Descriptions	M	Yes	
		3.4.1.5.2	Test Log - Activity and Event Entries	M	Yes	
		3.4.1.6.1	Test Anomaly Report Identifier	M	Yes	
		3.4.1.6.2	Test Anomaly Report - Date Anomaly Discovered	M	Yes	
		3.4.1.6.3	Test Anomaly Report - Context	M	Yes	
		3.4.1.6.4	Test Anomaly Report - Description of the Anomaly	M	Yes	
		3.4.1.6.5	Test Anomaly Report - Assessment of Urgency	M	Yes	
		3.4.1.6.6	Test Anomaly Report - Description of the Corrective Action	M	Yes	
		3.4.1.6.7	Test Anomaly Report - Conclusions and Recommendations	M	Yes	
		3.4.1.7.1	Conformance Summary	M	Yes	
		3.4.1.7.2	Summary of Testing Activities	M	Yes	
		3.4.1.7.3	Summary of Testing Task Results	M	Yes	
		3.4.1.7.4	Summary of Anomalies and Resolutions	M	Yes	
		3.4.1.7.5	Summary of Pass/Fail Results	M	Yes	
2.8.5		Requirements Verification Methods		O	Yes / No	
		3.4.1.4.1	Test Procedure Identifier	M	Yes	
		3.4.1.4.2	Test Case References	M	Yes	
		3.4.1.4.3	Requirements Verification Method(s)	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	User Need	FR ID	Functional Requirement	Conformance	Support	Additional Specifications
		3.4.1.4.4	Procedure Descriptions	M	Yes	
		3.4.1.4.5	Procedure Steps	M	Yes	
		3.4.1.4.6	Relationship to other Procedures	M	Yes	
		3.4.1.4.7	Procedure Special Requirements	M	Yes	
2.8.6	Test Cases			M	Yes	
		3.4.1.3.1	Test Case Identifier	M	Yes	
		3.4.1.3.2	Inputs	M	Yes	
		3.4.1.3.3	Outcomes	M	Yes	
		3.4.1.3.4	Feature Pass/Fail Criteria	M	Yes	
		3.4.1.3.5	Intercase Dependencies	M	Yes	
2.8.7	Test Coverage			O	Yes / No	
		3.4.1.2.1	Test Items	M	Yes	
		3.4.1.2.2	Features to be Tested	M	Yes	
		3.4.1.2.3	Features not to be Tested	M	Yes	
		3.4.1.2.4	Test Coverage	M	Yes	
		3.4.1.2.5	Item Pass/Fail Criteria	M	Yes	
		3.4.1.2.6	Requirements to Test Case Traceability Matrix	M	Yes	
		3.4.1.2.7	Organization Requirements	M	Yes	
		3.4.1.2.8	Roles and Responsibilities	M	Yes	
		3.4.1.2.9	Resources Summary	M	Yes	
		3.4.1.2.10	Test Schedule	M	Yes	
		3.4.1.2.11	Document Procedures and History	M	Yes	
2.8.8 (TestPro)	Test Procedures			O	Yes / No	
		3.4.1.4.1	Test Procedure Identifier	M	Yes	
		3.4.1.4.2	Test Case References	M	Yes	
		3.4.1.4.3	Requirements Verification Method(s)	M	Yes	
		3.4.1.4.4	Procedure Descriptions	M	Yes	
		3.4.1.4.5	Procedure Steps	M	Yes	
		3.4.1.4.6	Relationship to other Procedures	M	Yes	
		3.4.1.4.7	Procedure Special Requirements	M	Yes	
2.8.9	Identify Existing Test Documentation			O	Yes / No	
		Annex F.1	Existing Test Documentation	M	Yes	
2.8.10	Configuration and Change Management Needs			O	Yes / No	
		3.4.1.2.1	Test Items	M	Yes	

3.3 Requirements

The requirements for the CI Implementation Guide follow.

3.3.1 Architectural Requirements

The requirements for wireless communications between the connected intersections and the applications on an OBU/MU follows.

3.3.1.1 IEEE Std 802.11-2016 (DSRC)

A connected intersection shall exchange data with OBUs/MUs using *IEEE Std 802.11-2016* (operating outside the context of a BSS) in the 5.895 to 5.925 GHz band on channels 180, 182, and 184. Selection of channel is deployment dependent.

NOTE: Subject to change. This requirement is applicable only in the United States. The United States Federal Communications Commission (FCC) ruled only the upper 30 MHz will be available as of November 2020.

3.3.1.1.1 User Priority Levels

The requirements for User Priority Levels for transmitted messages follows.

3.3.1.1.1.1 User Priority Level – SPaT Message

A connected intersection shall broadcast SPaT messages with User Priority 7 (802.11 AC_VO).

3.3.1.1.1.2 User Priority Level – MAP Message

A connected intersection shall broadcast MAP messages with User Priority 3 (802.11 AC_BE).

3.3.1.1.1.3 User Priority Level – RTCMcorrections Message

A connected intersection shall broadcast RTCMcorrections messages with User Priority 5 (802.11 AC_VI).

3.3.1.2 3GPP PC5 Mode 4 (Release 14 or 15 (C-V2X))

A connected intersection shall exchange data with OBUs/MUs using 3GPP PC5 Mode 4 (V2X Sidelink) in the 5.905 to 5.925 GHz band with 20 MHz channel width (one channel – Channel 183).

3.3.1.2.1 ProSe Per Packet Priority (PPPP)

The requirements for ProSe Per Packet Priority for transmitted messages follows.

3.3.1.2.1.1 ProSe Per Packet Priority – SPaT Message

A connected intersection shall broadcast SPaT messages with PPPP 5.

Note: This setting is the recommended values in SAE J3161_202204.

3.3.1.2.1.2 ProSe Per Packet Priority – MAP Message

A connected intersection shall broadcast MAP messages with PPPP 3.

Note: This setting is the recommended values in SAE J3161_202204.

3.3.1.2.1.3 ProSe Per Packet Priority – RTCMcorrections Message

A connected intersection shall broadcast RTCMcorrections messages with PPPP 5.

Note: This setting is the recommended values in SAE J3161_202204.

3.3.1.2.2 One Shot Transmission

All messages shall be transmitted using the one-shot transmission method defined in SAE J3161_202204.

3.3.2 TSC Infrastructure to RSU Requirements

The requirements for a TSC infrastructure to provide signal timing information to an RSU follow.

3.3.2.1 TSC Infrastructure Signal Timing Data Requirements

The requirements for a TSC infrastructure to provide signal phase and timing data to an RSU follow.

3.3.2.1.1 SPaT Information Messages Requirements

The formats for a TSC infrastructure to provide "SPaT information messages" to an RSU follow. SPaT information messages contain the signal phase and timing data, such as timing and movement state information for each movement through an intersection, necessary to generate an SAE J2735_202007 SPaT message.

3.3.2.1.1.1 NTCIP 1202 v03A SPaT Information

A TSC infrastructure shall transmit a SPaT information message to an RSU in conformance with the applicable requirements in *NTCIP 1202 v03A*, Section 3.5.4.

3.3.2.1.1.2 TSCBM SPaT Information

A TSC infrastructure shall transmit a SPaT information message to an RSU in compliance with the Traffic Signal Controller Interface defined in Chapter 3 of the *V2I Hub Interface Control Document (ICD)*, March 2017. This information message is also known as the Traffic Signal Controller Broadcast Message (TSCBM).

3.3.2.1.1.3 SPaT Message

A TSC infrastructure shall transmit a UPER-encoded SAE J2735_202007 SPaT message to an RSU as an Immediate Forward message.

3.3.2.1.2 TSC Infrastructure SPaT Information Message Transmission Rate

A TSC infrastructure shall transmit a SPaT information message to an RSU at an average rate of 10 messages per second \pm 1 message per second measured over a 2-second period.

3.3.2.1.3 TSC Infrastructure SPaT Information Message Transmission Failure Threshold

A TSC infrastructure shall not exceed 0.3 seconds between transmissions of SPaT information messages.

NOTE: This threshold is set based on the *NEMA TS 2 -2016* Standard.

NOTE: This threshold may be used by an RSU to determine that there is a communications issue between the RSU and TSC infrastructure. This could be due to a failure of the TSC infrastructure itself.

3.3.2.1.4 TSC Infrastructure SPaT Information Average Message Update Latency

When state changes are sent to the cabinet outputs, the TSC shall transmit the corresponding SPaT information to an RSU within 200 milliseconds on average when measured over a 2 second period as measured between the controller's cabinet output and the controller's Ethernet output to the RSU.

NOTE: The 200 milliseconds average latency stated in this requirement is still being discussed within the TCI TF due to potential additional latencies of a supervisory device such as an external control local application (ECLA) that is considered a part of the TSC infrastructure.

3.3.2.1.5 TSC Infrastructure Processing Latency

When there is a change of demand for right-of-way, a TSC infrastructure shall process the input and generate a corresponding SPaT information message within 500 milliseconds of receipt of the cabinet input (including NTCIP commands).

3.3.2.2 Signal Timing Status Requirements

The requirements for a TSC infrastructure to provide signal timing status to an RSU follow.

3.3.2.2.1 TSC Infrastructure Manual Control Indication

A TSC infrastructure shall indicate in a SPaT information message when it is in operating under manual control.

3.3.2.2.2 TSC Infrastructure Stop Time Indication

When not in a flash condition, a TSC infrastructure shall indicate in a SPaT information message when it is operating under stop time.

3.3.2.2.3 TSC Infrastructure Cabinet Flash (Exception Flash) Indication

A TSC infrastructure shall indicate in a SPaT information message when the transportation field cabinet is in a signal flash condition invoked outside of the TSC (e.g., a fault, toggle switch, police panel).

3.3.2.2.4 TSC Infrastructure Controller Flash (Operational Flash) Indication

A TSC infrastructure shall indicate in a SPaT information message when it is in a signal flash condition invoked by the TSC (e.g., Automatic Flash, Start-Up Flash, Preemption Flash).

3.3.2.2.5 TSC Infrastructure Preemption Operation Indication

A TSC infrastructure shall indicate in a SPaT information message when it is in a preemption operation.

3.3.2.2.6 TSC Infrastructure Priority Operation Indication

A TSC infrastructure shall indicate in a SPaT information message when it is in a priority operation.

3.3.2.2.7 TSC Infrastructure Fixed Time Control Indication

A TSC infrastructure shall indicate in a SPaT information message when it is operating under fixed time control.

3.3.2.2.8 TSC Infrastructure Non-Fixed Time Control

A TSC infrastructure shall indicate in a SPaT information message when it is not operating under fixed time control.

Note: Non-fixed time control could refer to actuated signal control (including semi-actuation), or some hybrid forms used in traffic responsive control or adaptive control.

3.3.2.3 TSC Infrastructure RLVW Requirements

The requirements for a TSC infrastructure to provide support the RLVW application follow.

3.3.2.3.1 TSC Infrastructure Assured Green End Time (AGET)

The TSC infrastructure shall provide an AGET when the TSC infrastructure has determined a specific time to terminate a green signal indication.

3.3.2.3.2 TSC Infrastructure Assured Green Period (AGP)

The TSC infrastructure shall provide an AGP for each through movement approach to the intersection.

3.3.2.3.3 TSC Infrastructure Minimum End Time With AGP

When an OBU/MU is detected in a RLVW Detection Zone (RDZ), the associated through movement is in green and the TSC infrastructure is not terminating the movement; the TSC infrastructure shall provide a minimum end time for the movement that is greater than or equal to the current time plus the AGP.

3.3.3 Message Requirements

The requirements for a connected intersection broadcasting messages to OBUs/MUs follow.

3.3.3.1 Message Performance Requirements

The performance requirements for a connected intersection broadcasting messages to OBUs/MUs follow.

3.3.3.1.1 Uniform Message Requirements

The requirements to provide a consistent representation of the situation and operating conditions at a connected intersection follow.

3.3.3.1.1.1 SPaT Message - SAE J2735

A connected intersection shall transmit signal timing information using signal phase and timing (SPaT) messages that conform to SAE J2735_202007 (MSG_SignalPhaseAndTiming Message).

3.3.3.1.1.2 SPaT Message - Mandatory Data Elements

A connected intersection shall provide those data elements in the SAE J2735_202007 MSG_SignalPhaseAndTiming Message defined as mandatory.

3.3.3.1.1.3 SPaT Message - CI Mandatory Data Elements

A connected intersection shall provide those data elements in the SAE J2735_202007 MSG_SignalPhaseAndTiming Message defined as optional but necessary to fulfill the CI requirements, as indicated in the NRTM (See Table 6).

3.3.3.1.1.4 SPaT Message PSID

A connected intersection shall broadcast SPaT messages using a Provider Service Identifier (PSID) of 0x82 (0p80-02).

The IEEE PSID Public Listing can be found at <https://standards.ieee.org/products-programs/regauth/psid/public/>.

3.3.3.1.1.5 MAP Message - SAE J2735

A connected intersection shall transmit roadway geometry information using MAP messages that conform to SAE J2735_202007 (MSG_MapData).

3.3.3.1.1.6 MAP Message - Mandatory Data Elements

A connected intersection shall provide those data elements in the SAE J2735_202007 MSG_MapData that are defined as mandatory.

3.3.3.1.1.7 MAP Message - Required Data Elements

A connected intersection shall provide those data elements in the SAE J2735_202007 MSG_MapData that are defined as optional but necessary to fulfill the CI requirements, as indicated in the NRTM (See Table 6).

3.3.3.1.1.8 MAP Message PSID

A connected intersection shall broadcast MAP messages using a Provider Service Identifier (PSID) of 0x20-40-97 (0pE0-00-00-17).

The IEEE PSID Public Listing can be found at <https://standards.ieee.org/products-programs/regauth/psid/public/>.

3.3.3.1.1.9 RTCMcorrections Message - SAE J2735

A connected intersection shall transmit position corrections information using RTCMcorrections messages that conform to SAE J2735_202007 (MSG_RTCMcorrections).

3.3.3.1.1.10 RTCMcorrections Message - Mandatory Data Elements

A connected intersection shall provide those data elements in the SAE J2735_202007 MSG_RTCMcorrections that are defined as mandatory.

3.3.3.1.1.11 RTCMcorrections Message - Required Data Elements

A connected intersection shall provide those data elements in the SAE J2735_202007 MSG_RTCMcorrections that are defined as optional but necessary to fulfill the CI requirements, as indicated in the Table 11.

3.3.3.1.1.12 RTCMcorrections Message PSID

A connected intersection shall broadcast RTCMcorrections messages using a Provider Service Identifier (PSID) of 0x80 (0p80-00).

The IEEE PSID Public Listing can be found at <https://standards.ieee.org/products-programs/regauth/psid/public/>.

3.3.3.1.2 Robustness Requirements

The requirements for a connected intersection to operate under different degraded conditions follow.

3.3.3.1.2.1 Broadcast SPaT Message

If the RSU has received valid values from the TSC infrastructure about its status, a connected intersection shall broadcast a SPaT message. Valid values from the TSC infrastructure are properly formatted and within the permitted data ranges.

3.3.3.1.3 Concise Messages Requirements

The requirements to provide complete data describing the situation within the maximum message size supported by the communications stack follow.

3.3.3.1.3.1 Transport Message Size - WAVE

A connected intersection using WAVE Short Messages (WSM) to broadcast messages to OBUs/MUs shall have message sizes, in bytes, not to exceed the message size allowed by the transport used.

3.3.3.1.3.2 Concise MAP Message Requirements

The requirements for concise MAP messages follow.

3.3.3.1.3.2.1 Nodes by Offsets

A connected intersection shall define the location of a node describing the center of a lane at the intersection using offsets from a reference point or a previous node point.

3.3.3.1.3.2.2 Computed Lanes Requirements

The requirements for a computed lane follow. The attributes of a computed lane can be expressed by the attributes of a lane by translating the attributes of another lane at the intersection. The new lane is expressed as an offset from the first point of the referenced lane. These requirements reduce the bandwidth needed to define the new lane at the intersection; instead of transmitting a new sequence of offset values for a lane with the same attributes, only offset values and the lane number of the referenced lane is transmitted.

3.3.3.1.3.2.2.1 Computed Lane - Lane Identifier

A connected intersection shall provide the lane identifier of the referenced lane that a computed lane is based on. The attributes of the computed lane are based on the attributes of the referenced lane.

3.3.3.1.3.2.2.2 Computed Lane - X-Offset

A connected intersection shall provide the x-offset, in centimeters, between the first node point of the referenced lane and the first node point of the computed lane.

3.3.3.1.3.2.2.3 Computed Lane - Y-Offset

A connected intersection shall provide the y-offset, in centimeters, between the first node point of the referenced lane and the first node point of the computed lane.

3.3.3.1.3.2.2.4 Computed Lane - Angle

A connected intersection shall provide the angle of a computed lane relative to the first node point of the referenced lane.

3.3.3.1.4 Advanced Notification Requirements

The requirements to provide data far enough in advance of the intersection so the application on an OBU/MU can process the data in time to react to a situation follow.

3.3.3.1.4.1 Data Coverage - Every Lane

A connected intersection shall broadcast messages such that the messages can be received by OBUs/MUs units in each lane approaching the intersection.

3.3.3.1.4.2 Advanced Notification - Time

A connected intersection shall broadcast messages to a distance of at least 10 seconds at the 85th percentile speed or a speed equal to the posted or statutory speed limit plus 7 miles per hour (mph) before approaching vehicles would reach the stop line for each approaching lane. The value of 10 seconds is based on calculations on how quickly applications can process the data, considers how often messages are sent, and assumes some lost packets.

3.3.3.1.5 Timeliness Requirements

The requirements for indicating changes in state, timing and physical indications follow.

3.3.3.1.5.1 SPaT Message - Broadcast Periodicity

A connected intersection shall broadcast SPaT messages periodically at average rate of 10 messages per second +/- 1 message over a 10-second period.

3.3.3.1.5.2 SPaT Message - Broadcast Latency

A connected intersection shall broadcast SPaT messages that reflects the actual signal indications of the intersection within a latency of no more than 300 milliseconds.

3.3.3.1.5.3 MAP Message - Broadcast Periodicity

A connected intersection shall broadcast MAP messages periodically at an average rate of 1 message per second +/- 1 message over a 10-second period.

3.3.3.1.6 Quality Assurance Requirements

The requirements to provide quality information follow.

3.3.3.1.6.1 Completeness - SPaT Message

A connected intersection shall provide a SPaT message containing signal phase and timing information for all movements controlled by the TSC infrastructure and included in the associated MAP message.

3.3.3.1.6.2 Completeness - MAP Message

A connected intersection shall provide a MAP message describing all travel lanes where a movement traversing the intersection is permitted.

3.3.3.2 Generic Message Requirements

The requirements for a connected intersection transmitting data follow.

3.3.3.2.1 Time Accuracy

For messages that include time, a connected intersection shall utilize time that is accurate to within 10 milliseconds (ms) of Coordinated Universal Time (UTC).

3.3.3.2.2 Message Revision Requirements

The requirements if the data transmitted by a connected intersection is new follow.

3.3.3.2.2.1 SPaT Message - Revision Counter Increment

A connected intersection shall increment a revision counter by 1 whenever the value of any data element in the SPaT message, except for the timestamp, describing the signal phase and timing for that intersection changes.

3.3.3.2.2.2 SPaT Message - Revision Counter Not Increment

A connected intersection shall not increment a message counter if the value of no data element in the SPaT message, except for the timestamp, describing the signal phase and timing for that intersection changes.

3.3.3.2.2.3 MAP Message - Revision Counter Increment

A connected intersection shall increment a revision counter if the value of any data element in the MAP message other than the time stamp changes.

3.3.3.2.2.4 MAP Message - Revision Counter Not Increment

A connected intersection shall not increment a message counter if the value of no data element in the MAP message other than the time stamp changes.

3.3.3.2.2.5 MAP Message - Intersection Revision Counter Increment

A connected intersection shall increment a revision counter for the intersection description within a MAP message whenever any data element describing that intersection changes.

Since a MAP message may contain descriptions of more than one intersection, it is possible for the MAP message revision counter to increment but the intersection revision counter to not increment. This happens when a different intersection description in the MAP message changes but not this intersection description.

3.3.3.2.2.6 MAP Message - Intersection Revision Counter Not Increment

A connected intersection shall not increment a revision counter for an intersection description within a MAP message if no data element describing the intersection changes.

3.3.3.2.2.7 RTCMcorrections Message - Sequence Number Increment

A connected intersection shall increment a sequence number if there is a change in the corrections content in the RTCMcorrections message.

3.3.3.2.2.8 RTCMcorrections Message - Sequence Number Not Increment

A connected intersection shall not increment the sequence number if there is no change in the corrections content received from the RTCM base in the RTCMcorrections message other than the change in UTC time.

3.3.3.2.3 Timestamp Requirements

The requirements for a timestamp in messages transmitted by a connected intersection follow.

3.3.3.2.3.1 SPaT Message - Message Time Stamp

A connected intersection shall provide a timestamp indicating the minute of the year when the SPaT message was created.

3.3.3.2.3.2 SPaT Message - Intersection Time Stamp

A connected intersection shall provide a timestamp indicating the milliseconds within the current minute when the SPaT message was generated, for each intersection within the SPaT message.

3.3.3.3 Signal Timing Data Requirements

The requirements for signal timing data broadcasted by a connected intersection follow.

3.3.3.3.1 Intersection Identification Requirements

The requirements to provide a unique identifier for an intersection follow.

3.3.3.3.1.1 Intersection Signal Timing Information

A connected intersection shall provide signal timing information for one or more intersections.

3.3.3.3.1.2 Road Regulator Identifier

A connected intersection shall provide a road regulator identifier unique within North America.

3.3.3.3.1.3 Intersection Reference Identifier

A connected intersection shall provide an intersection reference identifier unique to a road regulator identifier.

3.3.3.3.2 Intersection Status Requirements

The requirements to provide the status of a connected intersection follow.

3.3.3.3.2.1 Manual Control

A connected intersection shall indicate whether it is operating under manual control.

3.3.3.3.2.2 Stop Time

A connected intersection shall indicate whether it is operating under stop time.

3.3.3.3.2.3 Failure Flash

A connected intersection shall indicate whether the intersection is in a signal flash condition invoked outside of the TSC (e.g., a fault, toggle switch, police panel).

3.3.3.3.2.4 Preemption

A connected intersection shall indicate whether it is in preemption operation.

3.3.3.3.2.5 Priority

A connected intersection shall indicate whether it is in priority operation.

3.3.3.3.2.6 Fixed Time

A connected intersection shall indicate whether it is operating under fixed time control.

3.3.3.3.2.7 Traffic Dependent Mode

A connected intersection shall indicate whether it is not operating in fixed time control.

3.3.3.3.2.8 Standby Mode

A connected intersection shall indicate whether it is in a signal flash condition invoked by the TSC infrastructure (e.g., TOD Flash, Start-Up Flash, Preemption Flash).

3.3.3.3.2.9 Failure Mode

A connected intersection shall indicate whether the TSC infrastructure has a problem or failure in operation.

3.3.3.3.2.10 Controller Off

A connected intersection shall indicate whether the TSC infrastructure is not providing valid data.

3.3.3.3.2.11 Recent MAP Update

A connected intersection shall indicate whether it has had a recent MAP message update.

3.3.3.3.2.12 New Lane IDs

A connected intersection shall indicate whether it has had a recent change in MAP assigned lane IDs or which revocable lanes are currently enabled.

3.3.3.3.2.13 No MAP Available

A connected intersection shall indicate when no valid MAP is available. A MAP is considered not available when any of the following conditions is true.

- If a connected intersection does not have a valid MAP message to broadcast

3.3.3.3.2.14 No SPaT Available

A connected intersection shall indicate when no valid SPaT information is available. SPaT information is considered not available under the following conditions:

- If an RSU has received no valid SPaT information message from the TSC infrastructure for more than 300 milliseconds. Valid values from the TSC infrastructure are properly formatted and within the permitted data ranges.

3.3.3.3.3 Current Movement State Requirements

The requirements for the current movement state of a signal group follow.

3.3.3.3.3.1 Current Movement State for a Signal Group

A connected intersection shall provide the current movement state for each signal group identified in the MAP message. The valid values for the current movement state for a signal group are defined by DE_MovementPhaseState in *SAE J2735_202007*.

3.3.3.3.3.2 Unknown Current Movement State for a Signal Group

If the TSC infrastructure does not provide a value for the current movement state for a signal group, a connected intersection shall use a value of unavailable, as defined by DE_MovementPhaseState in *SAE J2735_202007*.

3.3.3.3.3.3 Flashing Yellow Arrow Permissive Movement

At an intersection that uses a flashing yellow arrow to control a permissive movement as part of a protected/permissive turn, a connected intersection shall use the value of permissive-Movement-Allowed as the current movement state for the signal group when the flashing yellow arrow is active, as defined by DE_MovementPhaseState in *SAE J2735_202007*.

3.3.3.3.3.4 Protected and Permissive Clearance

A connected intersection shall use the value of protected-clearance or permissive-clearance as the current movement state of a signal group to correspond with the protected or permissive condition of the allowed movement immediately preceding the current (clearance) interval, as defined by DE_MovementPhaseState in *SAE J2735_202007*.

3.3.3.3.3.5 Resolve Protected Versus Permissive Movement

When an allowed movement controlled by a signal group is sometimes protected and sometimes permissive, such as a protected/permissive left turn, a connected intersection shall determine whether the currently allowed movement is protected or permissive and use the corresponding current movement state (protected-Movement-Allowed, permissive-Movement-Allowed) for the signal group, as defined by DE_MovementPhaseState in *SAE J2735_202007*.

3.3.3.3.3.6 Conflict Causes Permissive

When any allowed movement controlled by a signal group includes a maneuver in conflict with any other movement that is in a permitted or clearance state, a connected intersection shall use permissive-Movement-Allowed or permissive-clearance as the current movement state for the signal group, as defined by DE_MovementPhaseState in *SAE J2735_202007*. Examples include a green ball with an opposing green ball, and a green ball with a permitted pedestrian movement for a turn.

3.3.3.3.7 No Conflict Causes Protected

When an allowed movement controlled by a signal group includes no maneuver in conflict with any other vehicle, pedestrian, or bicycle movement that is in a permitted or clearance state, a connected intersection shall use protected-Movement-Allowed or protected-clearance as the current movement state for the signal group, as defined by DE_MovementPhaseState in *SAE J2735_202007*.

3.3.3.3.8 WALK State Enumeration (No Conflict)

When an allowed pedestrian movement has no conflict with a vehicle movement controlled by a signal group that is in a permitted or clearance state, a connected intersection shall use protected-Movement-Allowed as the current movement state for the pedestrian WALK interval, as defined by DE_MovementPhaseState in *SAE J2735_202007*. Examples of a WALK state with no conflict include leading pedestrian intervals or exclusive pedestrian interval (Barnes Dance).

3.3.3.3.9 WALK State Enumeration (Potential Conflict)

When an allowed pedestrian movement is in conflict with a vehicle movement controlled by a signal group that is in a permitted or clearance state, a connected intersection shall use permissive-Movement-Allowed as the current movement state for the pedestrian WALK interval, as defined by DE_MovementPhaseState in *SAE J2735_202007*. Examples of a WALK state with potential conflicts include vehicles turning right on green across the pedestrian crosswalk in a WALK state.

3.3.3.3.10 Flashing DON'T WALK State Enumeration

A connected intersection shall use the protected-clearance or permissive-clearance as the current movement state for the pedestrian Flashing DON'T WALK interval, as defined by DE_MovementPhaseState in *SAE J2735_202007*, to correspond with the protected or permissive condition of the allowed WALK movement immediately preceding the current (clearance) interval.

3.3.3.3.11 Steady DON'T WALK State Enumeration

A connected intersection shall use stop-And-Remain as the current movement state for the pedestrian Steady DON'T WALK interval, as defined by DE_MovementPhaseState in *SAE J2735_202007*.

3.3.3.3.12 Movement State for Signal Groups Identified

A connected intersection shall provide the current movement state for only signal groups identified in the MAP message. The connected intersection will not provide a movement state for any signal group not identified by the corresponding MAP message.

3.3.3.4 Next Movement State Requirements

The requirements for the next movement state of a signal group follow.

3.3.3.4.1 Next Movement State

A connected intersection shall provide the next (future) movement state to follow the current movement state for a signal group. The valid values for the next movement state for a signal group are defined by DE_MovementPhaseState in *SAE J2735_202007*.

3.3.3.4.2 Unknown Next Movement State

In a situation where a connected intersection cannot determine the next movement state, a connected intersection shall use unavailable as the next movement state for a signal group, as defined by DE_MovementPhaseState in *SAE J2735_202007*.

3.3.3.3.4.3 No Past State

A connected intersection shall not provide the state or timing for intervals that are already completed.

3.3.3.3.5 Time Change Details Requirements

The requirements for when the signal interval state for a signal group may change follow.

3.3.3.3.5.1 Time Change Details

A connected intersection shall provide time change details for each signal group identified in the MAP message.

3.3.3.3.5.2 Unknown Time Change Detail

If the TSC infrastructure does not provide a value for a mandatory time change detail element, a connected intersection shall use a value of unknown, as defined by DE_TimeMark in *SAE J2735_202007*.

NOTE: The value of DE_TimeMark indicating undefined changed from a value of 36001 in *SAE J2735_201603* to a value of 36111 in *SAE J2735_202007*.

3.3.3.3.5.3 Minimum End Time

A connected intersection shall provide the soonest time, in tenths of a second in the current or next hour, that the current and any future interval in the SPaT message for a signal group could end in the absence of unpredicted events such as preemption or priority calls.

For intervals that do not have a predetermined minimum end time (actuated operations), the connected intersection the minimum end time will be 0.1 seconds or greater beyond the current time for the current interval. For intervals that do have a predetermined minimum end time (fixed time control), the minimum end time is the predetermined minimum end time.

3.3.3.3.5.4 Maximum End Time

A connected intersection shall provide the latest time, in tenths of a second in the current or next hour, that the current and any future interval could end in the absence of unpredictable events such as preemption or priority calls.

For intervals that do have a predetermined end time (fixed time control), the maximum end time is equal to the minimum end time.

3.3.3.3.5.5 Unknown Maximum End Time

In a situation where a connected intersection cannot determine a latest end time, a connected intersection shall use a value of unknown, as defined by DE_TimeMark in *SAE J2735_202007*.

NOTE: The value of DE_TimeMark indicating undefined changed from a value of 36001 in *SAE J2735_201603* to a value of 36111 in *SAE J2735_202007*.

3.3.3.3.5.6 No Current Movement State Start Time

A connected intersection shall not provide the start time of the current movement state. Note: this prohibited time mark would be a past time and is not needed for RLVW. Prohibiting this data element for

currently timing intervals removes any ambiguity as to whether start time is intended as a past time or a future time.

3.3.3.3.5.7 Next Movement State Start Time

A connected intersection shall provide the start time, in tenths of a second in the current or next hour, of the next (future) movement state to follow the current movement state for a signal group. Note: this is a future time.

3.3.3.3.5.8 Next State Start Time Equals Current State Minimum End Time

A connected intersection shall provide a start time for the next (future) movement state that is the same as the soonest time the current movement state could end.

3.3.3.3.6 Next Allowed Movement Requirements

The requirements for when a movement at an intersection is next allowed to proceed (e.g., green, flashing yellow) follow.

3.3.3.3.6.1 Time of Next Allowed Movement

A connected intersection shall provide the estimated time, in tenths of a second in the current or next hour, that the current movement will next be in the permissive-Movement-Allowed or protected-Movement-Allowed (green) state in the absence of unpredictable events such as preemption or priority calls.

3.3.3.3.7 Enabled Lanes Indication

If the MAP message for the intersection includes lanes indicated as being revocable lanes, a connected intersection shall identify which revocable lanes are currently enabled.

3.3.3.3.8 SPaT Message - Accuracy

A connected intersection shall broadcast SPaT messages that accurately reflect the physical signal indications at the intersection.

3.3.3.4 Roadway Geometry Data Requirements

The requirements to provide information about travel lanes follow.

3.3.3.4.1 Intersection Geometry Requirements

The requirements to provide information about the lanes in and around an intersection follow.

3.3.3.4.1.1 Intersection Geometry Information

A connected intersection shall provide travel lane information for one or more intersections.

3.3.3.4.1.2 Intersection Geometry - Road Regulator Identifier

As part of the roadway geometry information, a connected intersection shall provide a road regulator identifier unique within North America.

3.3.3.4.1.3 Intersection Geometry - Intersection Identifier

As part of the roadway geometry information, a connected intersection shall provide an intersection reference identifier unique to a road regulator identifier.

3.3.3.4.1.4 Intersection Reference Point Requirements

The requirements for the location of an intersection reference point follow.

3.3.3.4.1.4.1 Intersection Reference Point - Position

A connection intersection shall select an intersection reference point located close enough to the first node point of all lanes associated with the intersection such that the offset can be represented using the DE_Offset_B16 in *SAE J2735_202007* (327.67 meters).

3.3.3.4.1.4.2 Intersection Reference Point - Description

A connected intersection shall provide the following information regarding an intersection reference point.

- a) Latitude, in 1/10th microdegrees, as defined by DE_Latitude in *SAE J2735_202007*
- b) Longitude, in 1/10th microdegrees, as defined by DE_Longitude in *SAE J2735_202007*
- c) Elevation in 10 centimeter units as defined by DE_Elevation in *SAE J2735_202007*

3.3.3.4.1.4.3 Intersection Reference Point Accuracy

A connected intersection shall provide an intersection reference point whose total accuracy is within +/- 0.2 meters of ground truth.

3.3.3.4.1.5 Default Lane Width

A connected intersection shall provide the default lane width, in centimeters, for all lanes associated with the intersection.

3.3.3.4.1.6 Lane Identifier

A connected intersection shall assign a lane identifier unique within the intersection for each lane at the intersection, as defined by DE_LaneID in *SAE J2735_202007*.

3.3.3.4.1.7 Center of Vehicle Lane Geometry

A connected intersection shall describe the geometry of the center of each vehicle lane approaching (ingress), departing (egress) and internal to (storage) the intersection.

3.3.3.4.1.8 Center of Crosswalk Lane Geometry

A connected intersection shall describe the geometry of the center of each crosswalk lane at the intersection.

3.3.3.4.1.9 Center of Pedestrian Landings Geometry

A connected intersection shall describe the geometry of the center of each pedestrian landing at the intersection.

3.3.3.4.1.10 Lane Description

A connected intersection shall describe the geometry of the center of each lane by identifying at least two node points that define at least one line segment depicting the center of the lane.

3.3.3.4.1.11 First Node Point - Ingress Vehicle Lane

A connected intersection shall describe the first node point at the upstream edge of the stop line of each ingress vehicle lane, with each subsequent node being farther from the intersection.

3.3.3.4.1.12 First Node Point - Egress Vehicle Lane

A connected intersection shall describe the first node point at the downstream edge of the crosswalk for each egress vehicle lane, with each subsequent node being farther from the intersection.

3.3.3.4.1.13 Node Offset from Intersection Reference Point

A connected intersection shall describe the location of first node point of a lane by providing an X (east-west) and a Y (north-south) offset, in centimeters, from the intersection reference point.

3.3.3.4.1.14 Node Elevation Offset from Intersection Reference Point

A connected intersection shall describe the elevation offset, in one centimeter units, of the first node point of a lane from the intersection reference point.

3.3.3.4.1.15 Offset from Previous Node

A connected intersection shall describe the location of a node subsequent to the first node point of a lane by providing an X (east-west) and a Y (north-south) offset, in centimeters, from the previous node point.

3.3.3.4.1.16 Elevation Offset from Previous Node

A connected intersection shall describe the elevation offset, in one centimeter units, of a node from the previous node point for a lane.

3.3.3.4.1.17 Advanced Notification - Ingress Vehicle Lane

A connected intersection shall describe node points of each ingress vehicle lane that extend a minimum distance upstream from the first node point of the lane 10 seconds at the 85th percentile speed or a speed equal to the posted or statutory speed limit plus 7 miles per hour (mph).

3.3.3.4.1.18 End Nodes - Crosswalk Lane

A connected intersection shall describe the first and last node point of a crosswalk lane at the edge of the curb.

3.3.3.4.1.19 End Nodes - Pedestrian Landing

A connected intersection shall describe the first and last node point of a pedestrian landing (essentially a sidewalk lane) at the edge of the curb, co-incident with the end nodes of the adjacent crosswalk lanes.

3.3.3.4.1.20 Maximum Distance between Nodes

When describing a lane with a horizontal curve, a connected intersection shall place the next node point within a distance such that the maximum distance between the actual centerline of a lane and a straight line between the two node points, does not exceed 0.5 meters. This concept is shown in Figure 13.

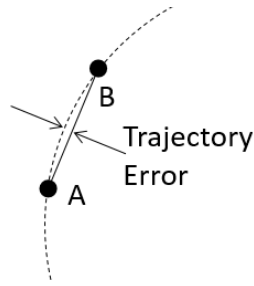


Figure 13. Trajectory Error.

3.3.3.4.1.21 Maximum Number of Nodes

A connected intersection shall describe the centerline of the path of a lane with no more than 63 node points.

3.3.3.4.1.22 Node Lane Width

If the width of a lane at a node point is different than the default lane width and the lane width at the preceding node, a connected intersection shall describe change in width of the lane, in centimeters, at the node position.

3.3.3.4.1.23 Node Accuracy

A connected intersection shall describe the absolute node position with an accuracy within ± 0.2 meters of the actual location of the node.

3.3.3.4.2 Lane Attributes

The requirements to describe the allowed us of a lane at an intersection follows.

3.3.3.4.2.1 Direction of Travel

A connected intersection shall identify the allowable direction(s) of travel for a lane, as defined by DE_LaneDirection in *SAE J2735_202007*.

3.3.3.4.2.2 Lane Sharing

A connected intersection shall identify the allowed user types that are permitted to use the lane, as defined by DE_LaneSharing in *SAE J2735_202007*.

3.3.3.4.2.3 Lane Type Attributes

A connected intersection shall identify the attribute information specific to a given lane type, as defined by DE_LaneTypeAttributes in *SAE J2735_202007*. The types of lanes are vehicle lane, crosswalk, bike lane, sidewalk, medians and channels, striped lanes, tracked lanes (for trains and trolleys), and parking lanes.

3.3.3.4.2.4 Lane Attributes - Vehicle

A connected intersection shall indicate the applicable attributes for a vehicle lane, as defined by DE_LaneAttributes-Vehicle in *SAE J2735_202007*. Examples of attributes are if the lane is a revocable lane, and any lane restrictions (HOV, Taxi, private use, etc.).

3.3.3.4.2.5 Lane Attributes - Crosswalk

A connected intersection shall indicate the applicable attributes for a crosswalk, as defined by DE_LaneAttributes-Crosswalk in *SAE J2735_202007*. Examples of attributes are if the lane is a revocable lane, and how the signal timing at the signalized intersection addresses travelers in the crosswalk lane.

3.3.3.4.2.6 Lane Attributes - Bicycle

A connected intersection shall indicate the applicable attributes for a bicycle lane, as defined by DE_LaneAttributes-Bike in *SAE J2735_202007*. Examples of attributes are if the lane is a revocable lane, and how the signal timing at the signalized intersection addresses travelers in the bicycle lane.

3.3.3.4.2.7 Lane Attributes - Tracked Vehicles

A connected intersection shall indicate the applicable attributes for a tracked vehicle lane, as defined by DE_LaneAttributes-TrackedVehicle in *SAE J2735_202007*. Examples of attributes are if the lane is a revocable lane, and the type of track (commuter rail, light rail, etc.).

3.3.3.4.2.8 Lane Attributes - Parking

A connected intersection shall indicate the applicable attributes for a parking lane, as defined by DE_LaneAttributes-Parking in *SAE J2735_202007*. Examples of attributes are if the lane is a revocable lane, and the type of parking (parallel, head in parking, do not park zone, private parking, etc.).

3.3.3.4.3 Lane Maneuvers

A connected intersection shall identify for a lane each maneuver that is allowed for that lane at the stop line for ingress lanes and at the first node point for the downstream lane, as defined by DE_AllowedManeuvers in *SAE J2735_202007*.

3.3.3.4.4 Connections Between Lanes

The requirements to describe connections between a lane entering or within an intersection, and the downstream lane at an intersection follow.

3.3.3.4.4.1 Lane Connections

A connected intersection shall identify each permitted connection between a lane and each downstream lane at the intersection.

NOTE: The downstream lane may be an egress or another ingress lane.

3.3.3.4.4.2 Connection Egress Lane

For each permitted connection between an ingress lane and another lane, a connected intersection shall identify the other lane to which the ingress lane connects.

3.3.3.4.4.3 Connection Maneuvers

For each permitted connection between an ingress lane and the downstream lane, a connected intersection shall identify the maneuver the connection allows. Examples of a maneuver include left turn, straight ahead, right turn on red, always yield, go after a full stop, etc.

3.3.3.4.4.4 Connection Signal Group

For each permitted connection between an ingress lane and the downstream lane, a connected intersection shall identify the SPaT signal group that provides traffic signal control for that connection.

3.3.3.4.4.5 Include Only Permitted Connections

A connected intersection shall only identify a connection between a lane and a downstream lane at the intersection if the movement represented by that connection is allowed at the intersection. If a permitted connection does not exist at an intersection, that connection is not included in the MAP message.

3.3.3.4.5 Speed Limit Information Requirements

The requirements to provide the speed limit for a lane at the intersection follows.

3.3.3.4.5.1 Default Speed Limit

A connected intersection shall provide the default posted or statutory maximum speed limit for general traffic, in units of 0.02 meters per second, for the intersection.

3.3.3.4.5.2 Change in Lane Speed Limit

A connected intersection shall provide the posted or statutory speed limit, in units of 0.02 meters per second, for the lane starting at the node.

3.3.3.4.6 Revocable Lanes

At intersections having lanes with usage that is different at different times, such as lanes that by time of day are reversible, have turn restrictions, or have parking restrictions, a connected intersection shall define in the MAP message separate lanes for each variation of usage and designate each as a revocable lane.

3.3.3.4.7 MAP Message - Accuracy

A connected intersection shall broadcast MAP messages that accurately reflect the physical location and dimensions of all travel lanes traversing the intersection within defined tolerances.

3.3.3.4.8 Signal Timing and Roadway Geometry Information Synchronization

The requirements to ensure that the roadway geometry information being broadcast reflect the current operating state used to generate the signal timing data follow.

3.3.3.4.8.1 Matching Intersection Reference Identifier

A connected intersection shall provide an intersection reference identifier for the SPaT message that matches the intersection reference identifier used in the MAP message for the same intersection. The intersection reference identifier consists of the road regulator identifier (See 3.3.3.3.1.2) and the intersection identifier (See 3.3.3.3.1.3).

3.3.3.4.8.2 Matching SPaT and MAP Version

The contents of the SPaT message broadcasted for an intersection shall be consistent/compatible with the MAP message broadcasted for the same intersection. For example, if the physical roadway geometry changes, the SPaT message may need to be updated to reflect those changes.

3.3.3.5 Positioning Messages

The requirements for positioning data broadcasted by a connected intersection follow.

3.3.3.5.1 Positioning Corrections

An RSU shall broadcast Radio Technical Commission for Maritime Services (RTCM) corrections per RTCM10403.3, and with Multiple Signals Messages (MSM) 4. The messages consist of the following:

- a) Station location message numbers 1005 or 1006. 1006 is preferred, but 1005 shall be used if 1006 is not available.
- b) The GNSS antenna and receiver location message 1033 (per the RTCM recommendation).
- c) The system parameter message 1013.
- d) The GPS MSM4 message 1074.
- e) If available, one of more of the following MSM4 messages: 1084 (GLONASS), 1094 (Galileo), and 1124 (BeiDou)

NOTE: In the United States, GLONASS is most commonly supported GNSS beyond GPS, so sending at least messages 1074 and 1084 is recommended.

NOTE: Vehicles may use other sources of correction or means for achieving the necessary precision.

3.3.3.5.2 Real-Time Kinematics Requirements

The requirements for to support real-time kinematics at a connected intersection follow.

3.3.3.5.2.1 RSU Proximity

The RTCM reference station providing correction messages shall be close enough to the RSU to provide adequate accuracy and latency.

NOTE: The RSU may have integrated RTCM capabilities, or the RTCM could be generated by a nearby station. The RSU should broadcast a calculated RTK if it is far from a surveyed reference station.

3.3.3.5.2.2 Minimum RTCM Corrections Broadcast Frequency

An RSU shall broadcast RTCM corrections to OBUs with sufficient range and frequency for vehicles to enable lane matching at a minimum of 10 seconds at the 85th percentile speed or a speed equal to the posted or statutory speed limit plus 7 miles per hour (mph) before approaching vehicles would reach the stop line for each approaching lane.

3.3.4 Security Requirements

The security requirements for a connected intersection follow.

3.3.4.1 Connected Intersection System Trustworthiness Requirements

The requirements for data trustworthiness for a connected intersection follow.

3.3.4.1.1 SPaT Information Message Trustworthiness - RSU

A connected intersection shall implement mechanisms to ensure that commands or data sent to the RSU result in the RSU sending SPaT messages that are consistent with SPaT information message received from the TSC infrastructure. These mechanisms consist of the following:

- Protection against bad firmware updates or installation of applications outside the firmware update process
- Protection against changes to configuration parameters that affect the contents of generated SPaT messages
- Enabling of RSU to determine in a timely fashion that no valid SPaT information message is available

3.3.4.1.2 SPaT Information Message Trustworthiness - TSC Infrastructure

A connected intersection shall implement mechanisms to ensure that commands or data sent to the TSC infrastructure result in the TSC infrastructure sending a SPaT information message to the RSU that is consistent with the actual signal behavior. These mechanisms consist of the following:

- Protection against bad firmware updates or installation of applications outside the firmware update process
- Protection against changes to configuration parameters that affect the output SPaT information message

3.3.4.1.3 MAP Data Trustworthiness

A connected intersection shall implement mechanisms to ensure that only MAP data from a trusted source is sent to the RSU for transmission.

NOTE: This may be achieved by, for example, signing the MAP at the point of generation (not the RSU), or by applying other data integrity and source authentication mechanisms to protect the MAP between the point of generation and the point of signing.

3.3.4.1.4 RTCM Corrections Data Trustworthiness

A connected intersection shall implement mechanisms to ensure that only RTCM corrections data from a trusted source is sent to the RSU for transmission.

3.3.4.2 Connected Intersection System Security Requirements

The requirements for network security of a connected intersection follow.

3.3.4.2.1 Secure Network

The center components that are part of a connected intersection shall be connected to a secure network supporting data integrity and confidentiality, source authentication, and authorization.

3.3.4.2.2 Assurance of Connection to Correct Network

The field components of a connected intersection shall support mechanisms by which they can obtain real-time assurances that they are connected to the correct network as intended by the connected intersection administrator.

3.3.4.3 Verification of Connected Intersection System Security Requirements

The requirements to provide verification of a connected intersection's compliance to system security requirements follow.

3.3.4.3.1 Security Compliance Assessment

The operating agency of a connected intersection (IOO) shall create *compliance assessment documentation* indicating how the system trustworthiness and system security requirements are to be fulfilled. For example, this documentation contains an attack tree with mitigations given for all identified attacks, showing the following:

- All attack methodologies and mitigations that might lead to the RSU transmitting incorrect SPaTs, and their mitigation, including the following:
 - All attack methodologies that might lead to the TSC infrastructure outputting incorrect SPaT information message, and their mitigation
- All attack methodologies and mitigations that might lead to the RSU transmitting incorrect MAPs, and their mitigation
- All attack methodologies vectors and mitigations that might lead to the RSU transmitting incorrect positioning corrections, and their mitigation

3.3.4.3.2 Point of Certification

A designated certification agent shall act as the decision maker whether security compliance assessment documentation is complete and correct in demonstrating network security, initially and periodically as per policy.

3.3.4.4 Certificate Issuing Requirements

The requirements for issuing device authentication certificates based on compliance assessment follow.

3.3.4.4.1 Certificate Issuance

Upon a positive decision of the compliance assessment, the SCMS provider shall note that the SPaT and MAP signers at a connected intersection are eligible to be issued certificates.

3.3.4.4.2 Certificate Nonissuance

If the compliance assessment fails to certify that the security requirements are fulfilled by a connected intersection system, the SCMS provider shall not (or no longer) issue any certificates to any devices within the connected intersection.

3.3.4.4.3 CI Operation Security Practices

A connected intersection shall satisfy a security policy which ties compliance to the documented network security/quality standards to a non-SCMS certificate authority issuing a client authentication certificate.

NOTE: A "connected intersection" in this context includes both the devices and the human operators of the connected intersection.

3.3.4.4.4 RSU Security Standards

An RSU shall comply with the documented network security/quality standards for a client or server authentication certificate.

3.3.4.4.5 TSC Infrastructure Security Standards

A TSC infrastructure shall comply with the documented network security/quality standards for a client authentication certificate.

3.3.4.5 Security Against Cyber Attack Requirements

Requirements for security against cyber attacks follow.

3.3.4.5.1 Cyber-Attack Recovery Plan

A connected intersection shall support a cyber-attack recovery plan for the connected intersection, that is continuously maintained to mitigate new and evolving threats.

NOTE: A “connected intersection” includes both the devices and the human operators of the connected intersection.

3.3.4.5.2 Cyber-Attack Robustness

A connected intersection shall maintain up to date access to a database of cyber-attacks relevant to any of the CI components as part of a cyber-attack robustness (i.e., resilience plus recovery) plan.

NOTE: the robustness plan may include both automated responses and human responses.

3.3.4.5.3 Network Protection

The IOO network shall implement measures, such as a firewall, to protect its individual networks and components from network-related attacks by monitoring connections to and from itself with the wider Internet.

3.3.4.6 Data Flow: Communications and Interface Security Requirements

The requirements for the security of data exchanges across each interface in the CI system follow.

3.3.4.6.1 Interface between RSU and TMS

The requirements for the security of data exchanges between an RSU and a TMS follow.

3.3.4.6.1.1 General RSU-TMS Interface Requirements

The general requirements for the security of data exchanges between an RSU and a TMS follow. These requirements describe secure protocols for the management of remote devices by which the RSU is managed by the TMS, running over a standards-based, secure transport protocol with mutual authentication of the identity of both RSU and TMS in terms of ownership and authorization, and with integrity and confidentiality protection of all data exchanged.

3.3.4.6.1.1.1 Secure Transport of SNMPv3

A TMS shall support use of SNMPv3 with TSM (Transport Security Model) security as defined in RFC 5991 to manage the RSU.

3.3.4.6.1.1.2 Use of (D)TLS for Management Protocols

Connections for *NTCIP 1218 v01* between the RSU and TMS shall be protected with Transport Layer Security (TLS) 1.2 or 1.3, or with Datagram Transport Layer Security (DTLS) 1.2 or 1.3. All other RSU to TMS connections shall be protected with TLS 1.3 or with DTLS 1.3 (as defined in IETF RFC 8446).

The RSU may act as a server role within the TLS or DLTS protocol.

SNMPv3 implemented by the RSU is currently defined over TLS 1.2. In the future, this is expected to change to TLS 1.3 or DTLS 1.3.

3.3.4.6.1.1.3 Use of SSH

Some RSU resources/properties may not be managed via SNMPv3 but via SSH 2.0. If a TMS uses SSH (RFC 4253) to manage an RSU via command-line interface, then the RSU shall implement account-based access control to prevent outsiders from gaining malicious access.

NOTE: This is a limited exception to requirement 3.3.4.6.1.1.2 above. The intent is to allow SSH for portions of *NTCIP 1218 v01* requiring its use for file transfer as well as to support certain administrative tasks not covered in *NTCIP 1218 v01*.

3.3.4.6.1.2 (D)TLS Certificate Requirements

TLS certificates follow the X.509 format. The requirements for TLS certificates for an RSU follow. The requirements for DLTS certificates are identical to the requirements for TLS certificates.

3.3.4.6.1.2.1 (D)TLS Authentication - Installation

An RSU shall support TLS client authentication solely via certificate.

3.3.4.6.1.2.2 (D)TLS Authentication - Rejection

If in a TLS server role, an RSU shall reject authentication attempts from a client presenting an untrusted certificate.

3.3.4.6.1.2.3 RSU Certificate Security

An RSU shall support secure installation and update of a (D)TLS certificate and associated private key for itself, to use as a server or as a client.

3.3.4.6.1.2.4 RSU Client Certificate Security

An RSU shall support secure installation, replacement and revocation of the (D)TLS client certificates and server certificates that it is expected to trust.

3.3.4.6.2 Interface between RSU and SCMS

An RSU shall adhere to the SCMS interface requirements as per the *RSU Standard v1.0* Section 3.3.5.10.3.1 SCMS Connectivity Requirements - CAMP or 3.3.5.10.3.2 SCMS Connectivity Requirement - IEEE Std 1609.2.1, as appropriate.

NOTE: the SCMS server (e.g., Registration Authority (RA)) is outside of the IOO traffic management network.

3.3.4.6.3 Interface between an RSU and the OBU/MU

The interface between an RSU and an OBU/MU shall be protected based on *IEEE Std 1609.2-2016* security profile for SPaT, MAP, and RTCM corrections messages.

NOTE: This is not a requirement that the RSU performs the signing, since the messages may be signed elsewhere.

3.3.4.6.4 Interface between an RSU and the TSC Infrastructure

The requirements for the security of data exchanges between an RSU and a TSC infrastructure follow.

3.3.4.6.4.1 Use of Secure Transport Protocol

The interface between an RSU and a TSC infrastructure shall use a secure transport protocol with mutual authentication of the identity of both the RSU and TSC infrastructure in terms of ownership and authorization, and integrity protection of all data exchanged.

NOTE: Confidentiality protection is not required but may be optionally applied.

3.3.4.6.4.2 Use of TLS Protocol

The interface between an RSU and a TSC infrastructure shall use TLS or DTLS with client certificate, where an RSU takes the role of the server or the client.

3.3.4.6.4.3 Protection against TSC Infrastructure Reconfiguration from the RSU

The TSC shall be protected against unauthorized accesses via the RSU interface to prevent reconfiguration of the TSC that may affect V2X application behavior in a way that was not intended (by a legitimate actor in the system).

3.3.4.6.4.4 Validation of Forwarded V2X Messages

If the RSU is configured to forward the Basic Safety Messages it receives from OBUs/MUs over the V2X interface to the TSC infrastructure, the RSU shall validate these messages in conformance with the requirements of the *RSU Standard v1.0*, Section 3.3.5.1.2 V2X Interface Security - Receiving and Forwarding Messages.

3.3.4.6.5 Interface between the TMS and the TSC Infrastructure

The interface between a TMS and a TSC infrastructure shall use a sufficiently secure protocol for remote management of devices, whereby the TMS manages the TSC infrastructure; for example, SNMPv3 over TLS.

3.3.4.6.6 Interface between the MAP Server and the TMS

The requirements for the security of data exchanges between a MAP Server and a TMS follow.

3.3.4.6.6.1 Secure Connection to MAP Server

A TMS shall establish a secure connection to a MAP server that is configured by the IOO.

This connection shall provide data integrity and confidentiality, as well as source authentication and authorization.

3.3.4.6.6.2 MAP Data Integrity

A MAP server shall ensure the integrity of the MAP data from the generation source to the entity that signs it.

3.3.4.6.6.3 MAP Data Signature

The data a MAP server sends to the TMS and the TMS forwards shall contain the *IEEE Std 1609.2-2016* signature.

3.3.4.6.7 Interface between MAP Server and the SCMS

A MAP Server shall connect securely to the SCMS in order to obtain *IEEE Std 1609.2-2016* certificates with appropriate permissions to sign MAP messages.

3.3.4.7 Correct Operations Requirements

The requirements to provide correct operations for a connected intersection follow.

3.3.4.7.1 Device Protection Requirements

The requirements to protect field components of a connected intersection from network attacks follow.

3.3.4.7.1.1 RSU Protection

An RSU shall support an IP-level firewall (e.g., iptables) supporting at a minimum the following:

- Closing all unused ports by default
The applicable requirement in *RSU Standard v1.0* is requirement 3.3.5.8.1 RSU OS Applications and Services
- Opening the *NTCIP 1218 v01* port for incoming connections only
The applicable requirement in *RSU Standard v1.0* is 3.3.5.8.2 RSU OS Ports and Protocols
- Blocking individual source IP addresses, for example if incoming connection requests from that address are repeatedly rejected by higher layers. NOTE: Goal is to throttle connection attempts to minimize the chance or impact of denial-of-service attacks.

3.3.4.7.1.2 Device Protection

A TMS shall employ mechanisms to protect itself against intrusions that would result in invalid or unauthorized data being sent to an RSU.

NOTE: Examples of such a mechanism is: support an IP-level firewall (e.g., iptables), at a minimum closing, of all unused ports by default and opening the *NTCIP 1218 v01* port for outgoing connections only.

3.3.4.7.2 Secure Administration of RSU

The requirements to provide secure administration of an RSU follow.

3.3.4.7.2.1 Secure RSU Administration User Interface

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

3.3.4.7.2.2 Password Change Prompt

An RSU shall prompt a user accessing an RSU for the first time to change the default password. The applicable requirement in *RSU Standard v01* is 3.3.5.8.3, RSU Password.

3.3.4.7.2.3 Remote Restart

An RSU shall support remote restart. The applicable requirement in *RSU Standard v01* is 3.3.2.2.1 Remote Restart.

3.3.4.7.2.4 Log Restarts

An RSU shall log all restart operations in an RSU's event log file. The applicable requirement in *RSU Standard v01* is 3.3.2.2.4 Log Restarts.

3.3.4.7.2.5 Factory Default

An RSU shall support a means to set an RSU back to the factory default locally. The applicable requirement in *RSU Standard v01* is 3.3.2.2.2 Factory Default.

3.3.4.7.2.6 Protection against Tampering

An RSU enclosure and ports shall support tamper evident mechanisms. The applicable requirement in *RSU Standard v01* is 3.3.5.6.1 Tamper Evident Enclosure - Visual Requirements and 3.3.5.6.2 Tamper Evident Unused Port Requirements.

3.3.4.7.2.7 Operational, Security and other Events Logging - RSU

An RSU shall record salient events in a non-volatile log, as defined in *RSU Standard v01*, 3.3.5.13, Logging for General and Security Purposes Requirement. This requirement is needed at least for diagnosis (e.g., of cyber attacks).

NOTE: This includes logging of security events such as authentication failures, logs of changes to its configuration.

3.3.4.7.2.8 Operational Logging - TMS

A TMS shall record salient events in a non-volatile log. This includes logging of security events such as authentication failures, logs of changes to its configuration.

3.3.4.7.2.9 Operational Logging - TSC Infrastructure

The TSC Infrastructure shall record salient events in a non-volatile log. This includes logging of security events such as authentication failures, logs of changes to its configuration.

3.3.4.7.2.10 Determine Mode of Operations

An RSU shall report its current mode of operations to an authorized actor using NTCIP 1218. The RSU modes of operations are the following: fully operational, standby (non-transmit) mode, and fault. The applicable requirement in *RSU Standard v01* is 3.3.3.2.1 Determine Mode of Operations.

3.3.4.7.2.11 Determine Operational Status

An RSU shall report its operational status using NTCIP 1218. The applicable requirement in *RSU Standard v01* is 3.3.3.2.2 Monitor Current Status.

3.3.4.7.2.12 Determine Operational Performance

An RSU shall report operational performance statistics of the RSU using NTCIP 1218. The applicable requirement in *RSU Standard v01* is 3.3.3.2.3 Determine Operational Performance.

3.3.4.7.2.13 Determine Operating Environment

An RSU shall report the operating environment around the RSU using NTCIP 1218. The applicable requirements in *RSU Standard v01* is 3.3.3.2.4 Determine Operating Environment.

3.3.4.7.2.14 Access Control Policy

An RSU shall support access control policy covering enabling assignment of what tasks an administrator is allowed to carry out. The RSU access control policy shall enforce administrator access rights.

3.3.4.7.3 RSU Device Class Requirement

An RSU device class shall be a “Class 3” device (defined in ARC-IT), namely a setting for Confidentiality, Integrity and Availability of Moderate, High, and Moderate respectively. That is, the RSU satisfies the following:

- Compliance with *NIST FIPS 140-2* Level 3 physical security requirements for an Hardware Security Module (HSM)
- Support for remote and physical management via SNMPv3, requiring role-remote authentication in both cases

3.3.4.7.4 TSC Device Class Requirement

A Traffic Signal Controller device class shall be a “Class 3” device (defined in ARC-IT), namely a setting for Confidentiality, Integrity, and Availability of Moderate, High, Moderate respectively. That is, the TSC satisfies the following:

- Compliance with *NIST FIPS 140-2* Level 3 physical security requirements for its HSM, if equipped with an HSM
- Support for remote and physical management via SNMPv3, requiring role-remote authentication in both cases

3.3.4.7.5 MAP Signer Device Class Requirement

A MAP Signing device shall be a “Class 3” device (defined in ARC-IT), namely a setting for Confidentiality, Integrity and Availability of Moderate, High, and Moderate respectively. That is, the MAP Signer satisfies the following:

- Compliance with *NIST FIPS 140-2* Level 3 physical security requirements for an HSM

3.3.4.7.6 Authenticated Secure Update Requirements

The requirements for secure updates of software and firmware follows.

3.3.4.7.6.1 RSU Software and Firmware Updates

An RSU shall support remote software and firmware updates in according with *RSU Standard v1.0* requirement 3.3.1.14 Software and Firmware Updates Requirements.

3.3.4.7.6.2 Trustworthiness of Software and Firmware Updates

An RSU shall only install software and firmware updates from a trusted source. Update packages shall be signed by the RSU manufacturer and authenticated by the RSU before installation. The RSU software update system shall protect software update keys from compromise.

3.3.4.7.6.3 TSC Infrastructure Software and Firmware Updates

If the TSC infrastructure software, ECLA, and/or firmware can be updated, the TSC infrastructure shall support mechanisms to securely update them either locally, remotely, or both.

3.3.4.8 Network Monitoring Requirements

An RSU shall report the network administration of unauthenticated or failed access attempts, and shall provide statistics of connection attempts.

3.3.4.9 Credential Management Requirements

The requirements for credentials management for a connected intersection follow.

3.3.4.9.1 Credential Provisioning – (D)TLS Requirements

The requirements for provisioning a component of a connected intersection with TLS or DTLS client or server certificates follow.

Note: This provisioning task is separate and independent from all the SCMS-related credential management in Section 3.3.4.9.3.

3.3.4.9.1.1 Start-up Initialization

A component of the connected intersection shall be placed into an initialization mode upon installation, whereby it is securely provisioned with credentials to authenticate to external entities and credentials to trust.

3.3.4.9.1.2 Credential Updates

A component of the connected intersection system shall support a mechanism to **securely** update all of its provisioned credentials, including updating the status of the credentials to trust.

3.3.4.9.2 Management of Untrustworthy Devices - TLS Requirements

The requirements for protecting the system against exchanging data with untrustworthy devices (i.e., devices that were at one point trustworthy but have been compromised in some sense) follow.

3.3.4.9.2.1 Monitor Certificate Status

A connected intersection shall verify the validity of the certificate of any device/entity/component to which the connected intersection connects.

For example, use [OCSP] stapling when running TLS 1.3, or download [CRLs].

3.3.4.9.2.2 Drop Connections

If an RSU or a TSC infrastructure finds that a device is or seeks to be connected to does not have a valid certificate, the CI device shall disconnect or drop the connection attempt to that other device. A certificate may be invalid because it has been revoked or is expired.

3.3.4.9.3 Credential System Access - SCMS Requirements

The requirements to support SCMS credentials follow.

3.3.4.9.3.1 Connectivity Requirement

An RSU shall support connecting to an approved SCMS as per *RSU Standard v1.0* requirement 3.3.5.10.3.1 SCMS Connectivity Requirement - CAMP, or *RSU Standard v1.0* requirement 3.3.5.10.3.2 SCMS Connectivity Requirement - IEEE Std 1609.2.1, as appropriate.

The MAP Data Server component in charge of signing MAP messages shall support connecting to an approved SCMS.

3.3.4.9.3.2 Download SCMS Files

An RSU shall download updated CRLs and SCMS files within a time frame indicated in the current stored CRL file, as in the *RSU Standard v1.0*, requirements 3.3.5.10.5.1 Download CRL Requirements - CAMP and 3.3.5.10.6.1 Download SCMS Files - CAMP; or 3.3.5.10.5.2, Download CRL Requirements – IEEE Std 1609.2.1, and 3.3.5.10.6.2 Download SCMS Files - IEEE 1609.2.1, as appropriate.

3.4 Testing and Conformance Management

3.4.1 Test Documentation

The requirements for test documentation for a connected intersection follow.

3.4.1.1 Test Documentation Overview [Informative]

The definitions for the various test documents are the following:

- **Test.** (A) A set of one or more test cases. (B) A set of one or more test procedures. (C) A set of one or more test cases and procedures. (adopted from IEEE Std 610.12-1990 [B3]) (D) The activity of executing (A), (B), and/or (C). [*IEEE Std 829-2008*. Section 3.1.39]
- **Testing.** (A) An activity in which a system or component is executed under specified conditions, the results are observed or recorded, and an evaluation is made of some aspect of the system or component. (B) To conduct an activity as in (A). [*IEEE Std 829-2008*. Section 3.1.46]
- **Test Case.** (A) A set of test inputs, execution conditions, and expected results developed for a particular objective, such as to exercise a particular program path or to verify compliance with a specific requirement. (B) Documentation specifying inputs, predicted results, and a set of execution conditions for a test item. (adopted from IEEE Std 610.12-1990 [B2]). [*IEEE Std 829-2008*. Section 3.1.41]
- **Test Plan.** (A) A document describing the scope, approach, resources, and schedule of intended test activities. It identifies test items, the features to be tested, the testing tasks, who will do each task, and any risks requiring contingency planning. (B) A document that describes the technical and management approach to be followed for testing a system or component. Typical contents identify the items to be tested, tasks to be performed, responsibilities, schedules, and required resources for the testing activity. [*IEEE Std 829-2008*. Section 3.1.49]
- **Test Procedure.** (A) Detailed instructions for the setup, execution, and evaluation of results for a given test case. (B) A document containing a set of associated instructions as in (A). (C) Documentation that specifies a sequence of actions for the execution of a test. (adopted from IEEE Std 982.1TM-2005 [B7]). [*IEEE Std 829-2008*. Section 3.1.50]

NOTE: See section 2.8.4 for a description of test documentation relationships.

3.4.1.2 Test Plan Requirements

A test plan is defined as: (A) A document describing the scope, approach, resources, and schedule of intended test activities. It identifies test items, the features to be tested, the testing tasks, who will do each task, and any risks requiring contingency planning. (B) A document that describes the technical and management approach to be followed for testing a system or component. Typical contents identify the items to be tested, tasks to be performed, responsibilities, schedules, and required resources for the testing activity. [*IEEE Std 829-2008*. Section 3.1.49]

A connected intersection test plan shall contain the following sections and structure.

3.4.1.2.1 Test Items

A connected intersection test plan shall identify the test items (interfaces, modules, software, or system) that are the object of testing. [*IEEE Std 829-2008*. Section 9.2.1]

3.4.1.2.2 Features to be Tested

A connected intersection test plan shall identify all software product or software-based system features and combinations of software or system features to be tested. [*IEEE Std 829-2008*. Section 9.2.3]

3.4.1.2.3 Features not to be Tested

A connected intersection test plan shall identify all features and known significant combinations of features that will not be tested and the rationale for exclusion. [*IEEE Std 829-2008*. Section 9.2.4]

3.4.1.2.4 Test Coverage

A connected intersection test plan shall specify the requirement(s) for test coverage. Test coverage is an indication of the degree to which the test item has been reached or “covered” by the test cases. [*IEEE Std 829-2008*. Section 9.4.3]

3.4.1.2.5 Item Pass/Fail Criteria

A connected intersection test plan shall specify the criteria to be used to determine whether each test item has passed or failed testing. This is commonly based on the number of anomalies found. For example, specify that all mandatory items pass for an item to pass. [*IEEE Std 829-2008*. Section 9.2.6]

- Message Level Testing
 - SPaT
 - MAP
 - RTCM
- End-to-End Testing
 - Test Point A to Test Point B
- Field Level Testing (Reference Implementation)

3.4.1.2.6 Requirements to Test Case Traceability Matrix

A connected intersection test plan shall specify both the necessary and the desired properties of the test environment and any relevant test data. This may include the physical characteristics of the facilities, including the hardware, the off-the-shelf software, the test support tools and databases, personnel (identifying their organizations as appropriate), and anything else needed to support the test. It includes the environment for setup before the testing, execution during the testing (including data capture), and any post-testing activities (e.g., data reduction and analysis). Also specify the level of security that must be provided for, and any safety issues related to, the testing facilities, software, and any proprietary components. It may include externally provided content topics (possibly provided by third parties) including systems and/or subsystems. Identify the source(s) for all of these needs. [*IEEE Std 829-2008*. Section 9.3.2]

3.4.1.2.7 Organization Requirements

A connected intersection test plan shall provide an overview of the organizational content topic(s) and responsibilities for testing tasks. Identify organizational components and their primary (they are the task leader) and secondary (they are not the leader, but providing support) test-related responsibilities. [*IEEE Std 829-2008*. Section 8.1.5.5]

3.4.1.2.8 Roles and Responsibilities

A connected intersection test plan shall identify the individuals or groups responsible for managing, designing, preparing, executing, witnessing, checking results, and for resolving the anomalies found. [IEEE Std 829-2008. Section 9.3.3]

3.4.1.2.9 Resources Summary

A connected intersection test plan shall summarize the test resources, including staffing, facilities, tools, and special procedural requirements (e.g., security, access rights, and documentation control). [IEEE Std 829-2008. Section 8.1.5.4]

3.4.1.2.10 Test Schedule

A connected intersection test plan shall describe the test activities within the project life cycle and milestones. Summarize the overall schedule of the testing tasks, identifying where task results feed back to the development, organizational, and supporting processes (e.g., quality assurance and configuration management). A connected intersection test plan shall describe the task iteration policy for the re-execution of test tasks and any dependencies. [IEEE Std 829-2008. Section 8.1.5.2]

3.4.1.2.11 Document Procedures and History

A connected intersection test plan shall specify the means for identifying, approving, implementing, and recording changes to the test plan. This may be recorded in an overall configuration management system that is documented in a Configuration Management Plan that is referenced here. The change procedures need to include a log of all of the changes that have occurred since the inception of the test plan. This may include a Document ID (every testing document should have a unique ID connected to the system project), version number (sequential starting with first approved version), description of document changes, reason for changes (e.g., audit comments, team review, system changes), name of person making changes, and role of person to document (e.g., document author, project manager, system owner). [IEEE Std 829-2008. Section 8.3.2]

3.4.1.3 Test Case Requirements

A test case is defined as (A) A set of test inputs, execution conditions, and expected results developed for a particular objective, such as to exercise a particular program path or to verify compliance with a specific requirement. (B) Documentation specifying inputs, predicted results, and a set of execution conditions for a test item. (adopted from IEEE Std 610.12-1990 [B2]). [IEEE Std 829-2008. Section 3.1.41]

A connected intersection test case shall contain the following sections and structure.

3.4.1.3.1 Test Case Identifier

A connected intersection test plan shall describe the unique identifier needed by each test case so that it can be distinguished from all other test cases. An automated tool may control the generation of the identifiers. [IEEE Std 829-2008. Section 11.2.1]

3.4.1.3.2 Inputs

A connected intersection test case shall specify each input required to execute each test case. Some inputs will be specified by value (with tolerances where appropriate), whereas others, such as constant tables or transaction files, will be specified by name. [IEEE Std 829-2008. Section 11.2.3]

3.4.1.3.3 Outcomes

A connected intersection test case shall specify all outputs and the expected behavior (e.g., response time) required of the test items and provide the exact value(s) (with tolerances where appropriate). [IEEE Std 829-2008. Section 11.2.4]

3.4.1.3.4 Feature Pass/Fail Criteria

A connected intersection test case shall specify the criteria to be used to determine whether the feature or feature combination has passed or failed. [IEEE Std 829-2008. Section 10.2.4]

3.4.1.3.5 Intercase Dependencies

A connected intersection test case shall list the identifiers of test cases that must be executed prior to this test case. The test case shall summarize the nature of the dependencies. If test cases are documented (in a tool or otherwise) in the order in which they need to be executed, the Intercase Dependencies for most or all of the cases may not be needed. [IEEE Std 829-2008. Section 11.2.7]

3.4.1.4 Test Procedure Requirements

A test procedure is defined as (A) Detailed instructions for the setup, execution, and evaluation of results for a given test case. (B) A document containing a set of associated instructions as in (A). (C) Documentation that specifies a sequence of actions for the execution of a test. (Adopted from IEEE Std 982.1TM-2005 [B7]). [IEEE Std 829-2008. Section 3.1.50]

The components of a test procedure follow.

3.4.1.4.1 Test Procedure Identifier

A connected intersection test procedure shall describe the unique identifier needed by each test procedure so that it can be distinguished from other test procedures. An automated tool may control the generation of the identifiers. [Adapted from IEEE Std 829-2008. Section 11.2.1]

3.4.1.4.2 Test Case References

A connected intersection test procedure shall include references to relevant sections of any applicable test item documentation (e.g., references to usage procedures). If this procedure executes test case(s), provide reference(s) for all of them. [IEEE Std 829-2008. Section 12.1.3]

3.4.1.4.3 Requirements Verification Method(s)

A connected intersection test procedure shall identify a method of verification applied in the test procedure. The verification method shall be one of the following:

- **Inspection.** Examination of the system using one of your five senses. This test method is used for verification through a visual comparison that the requirement has been satisfied. For example, the Vendor shall provide training on the troubleshooting of the system, including local intersection and central portions.
- **Demonstration.** Manipulation of the system to verify that the results are as planned or expected. This test method is used for a requirement that the system can demonstrate without external test equipment.
- **Analysis.** Verification of system using models, calculations and testing equipment. This test method is used for a requirement that is fulfilled indirectly through a logical conclusion or mathematical analysis of a result. For example, algorithms for congestion: the designer may need to show that the requirement is met through the analysis of count and occupancy calculations in software or firmware.

- **Test.** Verification of system using a controlled and predefined series of inputs to ensure specific and predefined outputs are produced. This test method is used for a requirement that requires some external piece of test equipment (such as logic analyzer or voltmeter).

3.4.1.4.4 Procedure Descriptions

A connected intersection test procedure shall contain high level descriptions of the test procedures.

3.4.1.4.4.1 Message Level Testing

A connected intersection test procedure shall contain Message Level Testing, which verifies the format, structure, and content of data against a data specification.

3.4.1.4.4.1.1 Positive Testing

Message level testing for a connected intersection test procedure shall consist of positive testing, which invokes a system function to verify a proper response outcome.

3.4.1.4.4.1.2 Negative Testing

Message level testing for a connected intersection test procedure shall consist of negative testing, which invokes a system error outcome to verify that the system responds properly to errors caused from testing inputs.

3.4.1.4.4.1.3 Boundary Testing

Message level testing for a connected intersection test procedure shall consist of boundary testing, which are constructed to test the inputs and outputs of a system at the extremes in terms of value and size ranges.

3.4.1.4.4.1.4 Referential Integrity Testing

Message level testing for a connected intersection test procedure shall consist of referential integrity testing, which verifies the referential integrity as defined in a data specification of two or more messages.

3.4.1.4.4.2 End-to-End Testing - Packet Capture Analysis-based Testing

A connected intersection test procedure shall contain Message Level Testing, which relies on analysis techniques to compare the synchronized time values from packet data captures at two defined test points.

3.4.1.4.4.3 Field Environment Testing

A connected intersection test procedure shall contain field environment testing.

3.4.1.4.5 Procedure Steps

A connected intersection test procedure shall include ordered description of the steps to be taken by each participant. The connected intersection test procedure consists of the activities below (as applicable) for each procedure; there may be one or multiple procedures in one Level Test Procedure document. The connected intersection test procedure shall include the degree to which the procedure steps can be varied and the process for determining the allowable degree of variation (if variance is allowed). [*IEEE Std 829-2008*, Section 12.2.2]. The steps cover the following:

- Pre-test Equipment Setup and Configuration Verification
 - Inventory of hardware, software, test tools
 - Diagram(s)

- Data Collection Management
 - Start Time / End Time
 - Frequency of Collection of Data Points
 - Data Format (specification) of Logged Data
 - Data synchronization time markers to match test point data
- Analysis Steps
 - Calculations
 - Inspection of Data
- Pass/Fail Determination
- Security Permissions for Hardware and Network Access
- SCMS (where applicable)

3.4.1.4.6 Relationship to other Procedures

A connected intersection test procedure shall describe any requirements it may have for other procedures. Some examples of requirements for other test procedures include that they execute: Before this one; concurrently with this one; subsequent to this one. [*IEEE Std 829-2008*. Section 12.1.4]

3.4.1.4.7 Procedure Special Requirements

A connected intersection test procedure shall identify all that is needed to execute the tests, including but not limited to test cases, databases, automated tools, and external and/or third-party systems. A connected intersection test procedure shall identify any special requirements that are necessary for the its execution. These may include prerequisite procedures, special skill requirements, and special environmental requirements. [*IEEE Std 829-2008*. Section 12.2.1]

3.4.1.5 Test Log Requirements

A connected intersection test log shall contain the following sections and structure.

3.4.1.5.1 Test Log - Descriptions

A connected intersection test log shall provide any general information that applies to all entries in the log (exceptions can be specifically noted in a log entry). The following information may be considered:

- Identify the items being tested
- Date and time of start and stop
- Name of the individual running the test
- Any issue that causes testing to halt

[*IEEE Std 829-2008*. Section 13.2.1]

3.4.1.5.2 Test Log - Activity and Event Entries

A connected intersection test log shall Record activities/events for each relevant detail, including the beginning and end of activities, and the occurrence date and time along with the identity of the author. [*IEEE Std 829-2008*. Section 13.2.2]

The details covered shall include:

- Context
 - Test Case Identifier
 - Test Procedure Identifier
- Start Date/Time
- **Procedure Results.** For each execution, create a record of the results (manually or automated by a tool). Record the success or failure of each test case. [*IEEE Std 829-2008*. Section 13.2.2.2]
 - Test Case Pass/Fail

- **Anomaly Report Identifiers.** Record the identifier of each test Anomaly Report, whenever one is opened. [*IEEE Std 829-2008*. Section 13.2.2.5]

3.4.1.6 Test Anomaly Report Requirements

A connected intersection test anomaly report shall contain the following sections and structure.

3.4.1.6.1 Test Anomaly Report Identifier

A connected intersection test anomaly report shall have unique identifications for anomaly reports.

3.4.1.6.2 Test Anomaly Report - Date Anomaly Discovered

A connected intersection test anomaly report shall record the date and time that the anomaly was first identified. [*IEEE Std 829-2008*. Section 14.2.2]

3.4.1.6.3 Test Anomaly Report - Context

A connected intersection test anomaly report shall identify the test items involved indicating their version/revision level. References to the appropriate Test Procedure, Test Case, and Test Log may be supplied. [*IEEE Std 829-2008*. Section 14.2.3]

3.4.1.6.4 Test Anomaly Report - Description of the Anomaly

A connected intersection test anomaly report shall provide a description of the anomaly. Indicate whether the anomaly is reproducible, and provide enough information to make it reproducible if it is. [*IEEE Std 829-2008*. Section 14.2.4]

For example, anomalies may pertain to:

- Hardware (Connections, Cabinet, Wiring, etc.)
- Software and Unit:
 - RSU Message Receiver
 - RSU
 - Traffic Signal Controller
 - Test Software
- Operator Error

3.4.1.6.5 Test Anomaly Report - Assessment of Urgency

A connected intersection test anomaly report shall provide an evaluation of the need for an immediate repair. See IEEE Std 1044-1993 [B13] for suggested categories. Most organizations have from three to five categories, where the most serious category means that the product is unusable, and the least serious is a cosmetic anomaly. Include any relevant risk analysis and conclusions about risk. Categories may include the following:

- Immediate
 - Software fix
 - Update project documentation
 - Operator Training
 - Testware fix
 - Outside vendor/Third Party
- Eventual
 - Software fix
 - Update project documentation
 - Operator Training
 - Testware fix

- Outside vendor/Third Party
- Deferred
 - Fix in later release
 - Waiver requested (reference)
- No fix
 - No problem found
 - Waiver requested (reference)
 - Fix not justifiable
 - Fix not identifiable
 - Obsolete

[*IEEE Std 829-2008*. Section 14.2.6]

3.4.1.6.6 Test Anomaly Report - Description of the Corrective Action

A connected intersection test anomaly report shall summarize the activities during the corrective action taken to resolve the reported anomaly. It may include the time, effort, and risk required for the fix(es), with the actual time and effort added after the fix is completed. The corrective action may be deferral or retirement of a duplicate. [*IEEE Std 829-2008*. Section 14.2.7]

3.4.1.6.7 Test Anomaly Report - Conclusions and Recommendations

A connected intersection test anomaly report shall specify any recommendations for changes to the development and/or testing processes and documentation that would help to prevent this kind of anomaly in the future. This may include identification of the source or injection point of the anomaly. [*IEEE Std 829-2008*. Section 14.2.9]

3.4.1.7 Conformance Summary Report Requirements

A connected intersection conformance summary report shall contain the following sections and structure.

3.4.1.7.1 Conformance Summary

A connected intersection conformance summary report shall identify the cumulative result of testing (Pass/Fail) as to whether a Connected Intersection is conformant with this CI Implementation Guide.

3.4.1.7.2 Summary of Testing Activities

A connected intersection conformance summary report shall provide an executive-level summary of all test activities performed in support of this release, increment, or version. The activities identified in this section of the report should correspond to the test activities described in the Test Plan. [*IEEE Std 829-2008*. Section 17.2.1]

3.4.1.7.3 Summary of Testing Task Results

A connected intersection conformance summary report shall provide an executive-level summary of all testing tasks performed in support of this release, increment, or version. The tasks identified in this section of the report should correspond to the test tasks described in the Test Plan. [*IEEE Std 829-2008*. Section 17.2.1] This section also references Summary of Pass/Fail Results.

3.4.1.7.4 Summary of Anomalies and Resolutions

A connected intersection conformance summary report shall provide a categorized summary of anomalies discovered during testing performed in support of this release, increment, or version. Provide separate summaries for those anomalies that are resolved and those that remain unresolved. [*IEEE Std 829-2008*. Section 17.2.1]

3.4.1.7.5 Summary of Pass/Fail Results

A connected intersection conformance summary report should be organized to include Test Item, Test Case, and Test Procedure.

Section 4

System Design Details [Normative]

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

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

Section 4 is intended for the following readers:

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

For the first four categories of readers, Section 4 is useful in understanding the details of this CI Implementation Guide. For these readers, Section 3.2.3 is particularly useful in preparing procurement specifications and assists in mapping the various rows of the NRTM table to the more detailed text contained within the other sections.

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

4.1 Tutorial [Informative]

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

- Design details that do not require additional explanation. Some requirements do not require additional details on how to fulfill the requirement - those requirements are identified by "No Further Design Details" in the RTM.
- Design details that can be found in another reference
- Design details that require additional guidance or explanation. These design details are found in Section 4.3.

4.2 Requirements Traceability Matrix

The Requirements Traceability Matrix (RTM) links the requirements as in Section 3.3 with the corresponding design details on the same line. Using this table, each requirement in Section 3.3 can thus be traced in a conformant way. Each requirement points to either other sections of the standard where the formal design details on how to fulfill the requirement is described, provides no additional design details because the requirement is self-explanatory, or points to a normative reference that fulfills the requirement. In the latter case, the design details necessary to fulfill the requirement is contained within the normative reference.

To conform to a requirement, a connected intersection shall implement the design details traced from that requirement.

4.2.1 Notation [Informative]

4.2.1.1 Functional Requirement Columns

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

4.2.1.2 Design Details

The "Design Details" column either provides a hyperlinked reference to a section number where the design details are defined within Section 4, provides an external, normative reference that provides the details on how to fulfill the requirement, or indicates "No Further Design Details" because no additional design information is necessary (i.e., the requirement is self-explanatory).

4.2.1.3 Additional Specifications

The "Additional Specifications" column may (and should) be used to provide additional notes and requirements or may be used by an implementer to provide any additional details about the implementation.

4.2.2 Instructions for Completing the RTM [Informative]

To find the conformant design content for a functional requirement, search for the requirement identification (section) number or functional requirement under the appropriate column. Next to the functional requirements column are columns that define the conformant design details that fulfill the requirement. The columns either reference a section within this standard describing how the requirement is to be fulfilled; points a normative reference describing how to fulfill the functional requirement; or indicates "No Further Design Details" because no additional design information is necessary. The "Additional Specifications" column provides additional notes or details about the design content.

4.2.3 Requirements Traceability Matrix (RTM) Table

Requirements Traceability Matrix (RTM)			
FR ID	Functional Requirement	Design Detail	Additional Specification
3.3	Requirements		
3.3.1	Architectural Requirements		
3.3.1.1	IEEE Std 802.11-2016 (DSRC)	See <i>IEEE Std 802.11-2016</i>	
3.3.1.1.1	User Priority Levels		
3.3.1.1.1.1	User Priority Level – SPaT Message	See <i>IEEE Std 802.11-2016</i>	
3.3.1.1.1.2	User Priority Level – MAP Message	See <i>IEEE Std 802.11-2016</i>	
3.3.1.1.1.3	User Priority Level – RTCMcorrections Message	See <i>IEEE Std 802.11-2016</i>	
3.3.1.2	3GPP PC5 Mode 4 (Release 14 or 15 (C-V2X))	See <i>3GPP TS 23.285</i>	
3.3.1.2.1	ProSe Per Packet Priority (PPPP)		
3.3.1.2.1.1	ProSe Per Packet Priority – SPaT Message	See <i>SAE J3161_202204</i> .	
3.3.1.2.1.2	ProSe Per Packet Priority – MAP Message	See <i>SAE J3161_202204</i> .	
3.3.1.2.1.3	ProSe Per Packet Priority – RTCMcorrections Message	See <i>SAE J3161_202204</i> .	
3.3.1.2.2	One Shot Transmission	See <i>SAE J3161_202204</i> .	
3.3.2	TSC Infrastructure to RSU Requirements		
3.3.2.1	TSC Infrastructure Signal Timing Data Requirements		
3.3.2.1.1	SPaT Information Messages Requirements		
3.3.2.1.1.1	NTCIP 1202 v03A <i>SPaT Information</i>	See 4.3.2.1.1.1, NTCIP 1202A v03 SPaT Information	
3.3.2.1.1.2	TSCBM SPaT Information	See 4.3.2.1.1.2, TSCBM SPaT Information	
3.3.2.1.1.3	SPaT Message	See 4.3.2.1.1.3, SPaT Message	
3.3.2.1.2	TSC Infrastructure SPaT Information Message Transmission Rate	No Further Design Details	

Requirements Traceability Matrix (RTM)			
FR ID	Functional Requirement	Design Detail	Additional Specification
3.3.2.1.3	TSC Infrastructure SPaT Information Message Transmission Failure Threshold	No Further Design Details	
3.3.2.1.4	TSC Infrastructure SPaT Information Average Message Update Latency	No Further Design Details	
3.3.2.1.5	TSC Infrastructure Processing Latency	No Further Design Details	
3.3.2.2	Signal Timing Status Requirements		
3.3.2.2.1	TSC Infrastructure Manual Control Indication	See 4.3.2.2.1, TSC Infrastructure Manual Control Indication	
3.3.2.2.2	TSC Infrastructure Stop Time Indication	See 4.3.2.2.2, TSC Infrastructure Stop Time Indication	
3.3.2.2.3	TSC Infrastructure Cabinet Flash (Exception Flash) Indication	See 4.3.2.2.3, TSC Infrastructure Cabinet Flash (Exception Flash) Indication	
3.3.2.2.4	TSC Infrastructure Controller Flash (Operational Flash) Indication	See 4.3.2.2.4, TSC Infrastructure Controller Flash (Operational Flash) Indication	
3.3.2.2.5	TSC Infrastructure Preemption Operation Indication	See 4.3.2.2.5, TSC Infrastructure Preemption Operation Indication	
3.3.2.2.6	TSC Infrastructure Priority Operation Indication	See 4.3.2.2.6, TSC Infrastructure Priority Operation Indication	
3.3.2.2.7	TSC Infrastructure Fixed Time Control Indication	See 4.3.2.2.7, TSC Infrastructure Fixed Time Control Indication	
3.3.2.2.8	TSC Infrastructure Non-Fixed Time Control	See 4.3.2.2.8, TSC Infrastructure Non-Fixed Time Control	
3.3.2.3	TSC Infrastructure		
3.3.2.3.1	TSC Infrastructure Assured Green End Time (AGET)	See 4.3.2.3.1, TSC Infrastructure Assured Green End Time (AGET) Design	
3.3.2.3.2	TSC Infrastructure Assured Green Period	See 4.3.2.3.2, TSC Infrastructure Assured Green Period (AGP) Design Details	
3.3.2.3.3	TSC Infrastructure Minimum End Time With AGP	See 4.3.2.3.3, TSC Infrastructure Minimum End Time with AGP Design Details	
3.3.3	Message Requirements		
3.3.3.1	Message Performance Requirements		
3.3.3.1.1	Uniform Message Requirements		

Requirements Traceability Matrix (RTM)			
FR ID	Functional Requirement	Design Detail	Additional Specification
3.3.3.1.1.1	SPaT Message - SAE J2735	See MSG_SignalPhaseAndTiming Message (SPaT) in SAE J2735_202007	
3.3.3.1.1.2	SPaT Message - Mandatory Data Elements	See MSG_SignalPhaseAndTiming Message (SPaT) in SAE J2735_202007	
3.3.3.1.1.3	SPaT Message - CI Mandatory Data Elements	See 4.3.3.1.1.3, SPaT Message - CI Mandatory Data Element Design Details	
3.3.3.1.1.4	SPaT Message PSID	See 4.3.3.1.1.4, SPaT Message PSID	
3.3.3.1.1.5	MAP Message - SAE J2735	See MSG_MapData (MAP) in SAE J2735_202007.	
3.3.3.1.1.6	MAP Message - Mandatory Data Elements	See MSG_MapData (MAP) in SAE J2735_202007.	
3.3.3.1.1.7	MAP Message - Required Data Elements	See 4.3.3.1.1.7, MAP Message - Required Data Elements	
3.3.3.1.1.8	MAP Message PSID	See 4.3.3.1.1.8, MAP Message PSID	
3.3.3.1.1.9	RTCMcorrections Message - SAE J2735	See MSG_RTCMcorrections (RTCM) in SAE J2735_202007	
3.3.3.1.1.10	RTCMcorrections Message - Mandatory Data Elements	See MSG_RTCMcorrections (RTCM) in SAE J2735_202007	
3.3.3.1.1.11	RTCMcorrections Message - Required Data Elements	See 4.3.3.1.1.11, RTCMcorrections Message - Required Data Elements	
3.3.3.1.1.12	RTCMcorrections Message PSID	See 4.3.3.1.1.12, RTCMcorrections Message PSID	
3.3.3.1.2	Robustness Requirements		
3.3.3.1.2.1	Broadcast SPaT Message	See 4.3.3.1.2.1, Broadcast SPaT Message Design Details	
3.3.3.1.3	Concise Messages Requirements		
3.3.3.1.3.1	Transport Message Size - WAVE	See 4.3.3.1.3.1, Transport Message Size - WAVE	
3.3.3.1.3.2	Concise MAP Message Requirements		
3.3.3.1.3.2.1	Nodes by Offsets	See 4.3.3.1.3.2.1, Nodes by Offsets	
3.3.3.1.3.2.2	Computed Lanes Requirements		
3.3.3.1.3.2.2.1	Computed Lane - Lane Identifier	See 4.3.3.1.3.2.2.1, Computed Lane - Lane Identifier	
3.3.3.1.3.2.2.2	Computed Lane - X-Offset	See 4.3.3.1.3.2.2.2, Computed Lane - X-Offset	
3.3.3.1.3.2.2.3	Computed Lane - Y-Offset	See 4.3.3.1.3.2.2.3, Computed Lane - Y-Offset	
3.3.3.1.3.2.2.4	Computed Lane - Angle	See 4.3.3.1.3.2.2.4, Computed Lane - Angle	
3.3.3.1.4	Advanced Notification Requirements		
3.3.3.1.4.1	Data Coverage - Every Lane	See 4.3.3.1.4.1, Data Coverage - Every Lane	

Requirements Traceability Matrix (RTM)			
FR ID	Functional Requirement	Design Detail	Additional Specification
3.3.3.1.4.2	Advanced Notification - Time	See 4.3.3.1.4.2, Advanced Notification - Time	
3.3.3.1.5	Timeliness Requirements		
3.3.3.1.5.1	SPaT Message - Broadcast Periodicity	No Further Design Details	
3.3.3.1.5.2	SPaT Message - Broadcast Latency	See 4.3.3.1.5.2, SPaT Message - Broadcast Latency	
3.3.3.1.5.3	MAP Message - Broadcast Periodicity	No Further Design Details	
3.3.3.1.6	Quality Assurance Requirements		
3.3.3.1.6.1	Completeness - SPaT Message	See 4.3.3.1.6.1, Completeness - SPaT Message	
3.3.3.1.6.2	Completeness - MAP Message	See 4.3.3.1.6.2, Completeness - MAP Message	
3.3.3.2	Generic Message Requirements		
3.3.3.2.1	Time Accuracy	See 4.3.3.2.1, Time Accuracy	
3.3.3.2.2	Message Revision Requirements		
3.3.3.2.2.1	SPaT Message - Revision Counter Increment	See 4.3.3.2.2.1, SPaT Message - Revision Counter Increment	
3.3.3.2.2.2	SPaT Message - Revision Counter Not Increment	See 4.3.3.2.2.2, SPaT Message - Revision Counter Not Increment	
3.3.3.2.2.3	MAP Message - Revision Counter Increment	See 4.3.3.2.2.3, MAP Message - Revision Counter Increment	
3.3.3.2.2.4	MAP Message - Revision Counter Not Increment	See 4.3.3.2.2.4, MAP Message - Revision Counter Not Increment	
3.3.3.2.2.5	MAP Message - Intersection Revision Counter Increment	See 4.3.3.2.2.5, MAP Message - Intersection Revision Counter Increment	
3.3.3.2.2.6	MAP Message - Intersection Revision Counter Not Increment	See 4.3.3.2.2.6, MAP Message - Intersection Revision Counter Not Increment	
3.3.3.2.2.7	RTCMcorrections Message - Sequence Number Increment	See 4.3.3.2.2.7, RTCMcorrections Message - Sequence Number Increment	
3.3.3.2.2.8	RTCMcorrections Message - Sequence Number Not Increment	See 4.3.3.2.2.8, RTCMcorrections Message - Sequence Number Not Increment	
3.3.3.2.3	Timestamp Requirements		
3.3.3.2.3.1	SPaT Message - Message Time Stamp	See timestamp (DE_MinuteOfTheYear) for MSG_SignalPhaseAndTiming Message in SAE J2735_202007	
3.3.3.2.3.2	SPaT Message - Intersection Time Stamp	See 4.3.3.2.3.2, SPaT Message - Intersection Time Stamp	

Requirements Traceability Matrix (RTM)			
FR ID	Functional Requirement	Design Detail	Additional Specification
3.3.3.3	Signal Timing Data Requirements		
3.3.3.3.1	Intersection Identification Requirements		
3.3.3.3.1.1	Intersection Signal Timing Information	See intersections (DF_IntersectionStateList) for MSG_SignalPhaseAndTiming Message in <i>SAE J2735_202007</i>	
3.3.3.3.1.2	Road Regulator Identifier	See 4.3.3.3.1.2, Road Regulator Identifier	
3.3.3.3.1.3	Intersection Reference Identifier	See 4.3.3.3.1.3, Intersection Reference Identifier	
3.3.3.3.2	Intersection Status Requirements		
3.3.3.3.2.1	Manual Control	See 4.3.3.3.2.1, Manual Control	
3.3.3.3.2.2	Stop Time	See 4.3.3.3.2.2, Stop Time	
3.3.3.3.2.3	Failure Flash	See 4.3.3.3.2.3, Failure Flash	
3.3.3.3.2.4	Preemption	See 4.3.3.3.2.4, Preemption	
3.3.3.3.2.5	Priority	See 4.3.3.3.2.5, Priority	
3.3.3.3.2.6	Fixed Time	See 4.3.3.3.2.6, Fixed Time	
3.3.3.3.2.7	Traffic Dependent Mode	See 4.3.3.3.2.7, Traffic Dependent Mode	
3.3.3.3.2.8	Standby Mode	See 4.3.3.3.2.8, Standby Mode	
3.3.3.3.2.9	Failure Mode	See 4.3.3.3.2.9, Failure Mode	
3.3.3.3.2.10	Controller Off	See 4.3.3.3.2.10, Controller Off	
3.3.3.3.2.11	Recent MAP Update	See 4.3.3.3.2.11, Recent MAP Update	
3.3.3.3.2.12	New Lane IDs	See 4.3.3.3.2.12, New Lane IDs	
3.3.3.3.2.13	No MAP Available	See 4.3.3.3.2.13, No MAP Available	
3.3.3.3.2.14	No SPaT Available	See 4.3.3.3.2.14, No SPaT Available	
3.3.3.3.3	Current Movement State Requirements		
3.3.3.3.3.1	Current Movement State for a Signal Group	See 4.3.3.3.3.1, Current Movement State for a Signal Group	
3.3.3.3.3.2	Unknown Current Movement State for a Signal Group	See 4.3.3.3.3.2, Unknown Current Movement State for a Signal Group	
3.3.3.3.3.3	Flashing Yellow Arrow Permissive Movement	See 4.3.3.3.3.3, Flashing Yellow Arrow Permissive Movement	
3.3.3.3.3.4	Protected and Permissive Clearance	See 4.3.3.3.3.4, Protected and Permissive Clearance	
3.3.3.3.3.5	Resolve Protected Versus Permissive Movement	See 4.3.3.3.3.5, Resolve Protected Versus Permissive Movement	

Requirements Traceability Matrix (RTM)			
FR ID	Functional Requirement	Design Detail	Additional Specification
3.3.3.3.3.6	Conflict Causes Permissive	See 4.3.3.3.3.6, Conflict Causes Permissive	
3.3.3.3.3.7	No Conflict Causes Protected	See 4.3.3.3.3.7, No Conflict Causes Protected	
3.3.3.3.3.8	WALK State Enumeration (No Conflict)	See 4.3.3.3.3.8, WALK State Enumeration (No Conflict)	
3.3.3.3.3.9	WALK State Enumeration (Potential Conflict)	See 4.3.3.3.3.9, WALK State Enumeration (Potential Conflict)	
3.3.3.3.3.10	Flashing DON'T WALK State Enumeration	See 4.3.3.3.3.10, Flashing DON'T WALK State Enumeration	
3.3.3.3.3.11	Steady DON'T WALK State Enumeration	See 4.3.3.3.3.11, Steady DON'T WALK State Enumeration	
3.3.3.3.3.12	Movement State for Signal Groups Identified	No Further Design Details	
3.3.3.3.4	Next Movement State Requirements		
3.3.3.3.4.1	Next Movement State	See 4.3.3.3.4.1, Next Movement State	
3.3.3.3.4.2	Unknown Next Movement State	See 4.3.3.3.4.2, Unknown Next Movement State	
3.3.3.3.4.3	No Past State	No Further Design Details	
3.3.3.3.5	Time Change Details Requirements		
3.3.3.3.5.1	Time Change Details	See 4.3.3.3.5.1, Time Change Details	
3.3.3.3.5.2	Unknown Time Change Detail	See 4.3.3.3.5.2, Unknown Time Change Detail	
3.3.3.3.5.3	Minimum End Time	See 4.3.3.3.5.3, Minimum End Time	
3.3.3.3.5.4	Maximum End Time	See 4.3.3.3.5.4, Maximum End Time	
3.3.3.3.5.5	Unknown Maximum End Time	See 4.3.3.3.5.2, Unknown Time Change Detail	
3.3.3.3.5.6	No Current Movement State Start Time	No Further Design Details	
3.3.3.3.5.7	Next Movement State Start Time	See 4.3.3.3.5.7, Next Movement State Start Time	
3.3.3.3.5.8	Next State Start Time Equals Current State Minimum End Time	See 4.3.3.3.5.8, Next State Time Start Equals Current State Minimum End Time	
3.3.3.3.6	Next Allowed Movement Requirements		
3.3.3.3.6.1	Time of Next Allowed Movement	See 4.3.3.3.6.1, Time of Next Allowed Movement	
3.3.3.3.7	Enabled Lanes Indication	See 4.3.3.3.7, Enabled Lanes Indication	
3.3.3.3.8	SPaT Message - Accuracy	No Further Design Details	
3.3.3.4	Roadway Geometry Data Requirements		
3.3.3.4.1	Intersection Geometry Requirements		

Requirements Traceability Matrix (RTM)			
FR ID	Functional Requirement	Design Detail	Additional Specification
3.3.3.4.1.1	Intersection Geometry Information	See intersections (DF_IntersectionGeometryList) for MSG_MapData in <i>SAE J2735_202007</i>	
3.3.3.4.1.2	Intersection Geometry - Road Regulator Identifier	See 4.3.3.4.1.2, Intersection Geometry - Road Regulator Identifier	
3.3.3.4.1.3	Intersection Geometry - Intersection Identifier	See 4.3.3.4.1.3, Intersection Geometry - Intersection Identifier	
3.3.3.4.1.4	Intersection Reference Point Requirements		
3.3.3.4.1.4.1	Intersection Reference Point - Position	See 4.3.3.4.1.4.1, Intersection Reference Point - Position	
3.3.3.4.1.4.2	Intersection Reference Point - Description	See 4.3.3.4.1.4.2, Intersection Reference Point - Description	
3.3.3.4.1.4.3	Intersection Reference Point Accuracy	See 4.3.3.4.1.4.3, Intersection Reference Point Accuracy	
3.3.3.4.1.5	Default Lane Width	See 4.3.3.4.1.5, Default Lane Width	
3.3.3.4.1.6	Lane Identifier	See 4.3.3.4.1.6, Lane Identifier	
3.3.3.4.1.7	Center of Vehicle Lane Geometry	See 4.3.3.4.1.7, Center of Vehicle Lane Geometry	
3.3.3.4.1.8	Center of Crosswalk Lane Geometry	See 4.3.3.4.1.8, Center of Crosswalk Lane Geometry	
3.3.3.4.1.9	Center of Pedestrian Landings Geometry	See 4.3.3.4.1.9, Center of Pedestrian Landings Geometry	
3.3.3.4.1.10	Lane Description	See 4.3.3.4.1.10, Lane Description	
3.3.3.4.1.11	First Node Point - Ingress Vehicle Lane	See 4.3.3.4.1.11, First Node Point - Ingress Vehicle Lane Design Details	
3.3.3.4.1.12	First Node Point - Egress Vehicle Lane	See 4.3.3.4.1.12, First Node Point - Egress Vehicle Lane Design Details	
3.3.3.4.1.13	Node Offset from Intersection Reference Point	See 4.3.3.4.1.13, Node Offset from Intersection Reference Point	
3.3.3.4.1.14	Node Elevation Offset from Intersection Reference Point	See 4.3.3.4.1.14, Node Elevation Offset from Intersection Reference Point	
3.3.3.4.1.15	Offset from Previous Node	See 4.3.3.4.1.15, Offset from Previous Node	
3.3.3.4.1.16	Elevation Offset from Previous Node	See 4.3.3.4.1.16, Elevation Offset from Previous Node	
3.3.3.4.1.17	Advanced Notification - Ingress Vehicle Lane	See 4.3.3.4.1.17, Advanced Notification - Ingress Vehicle Lane	
3.3.3.4.1.18	End Nodes - Crosswalk Lane	See 4.3.3.4.1.18, End Nodes - Crosswalk Lane	
3.3.3.4.1.19	End Nodes - Pedestrian Landing	See 4.3.3.4.1.19, End Nodes - Pedestrian Landing	

Requirements Traceability Matrix (RTM)			
FR ID	Functional Requirement	Design Detail	Additional Specification
3.3.3.4.1.20	Maximum Distance between Nodes	See 4.3.3.4.1.20, Maximum Distance between Nodes	
3.3.3.4.1.21	Maximum Number of Nodes	See 4.3.3.4.1.21, Maximum Number of Nodes	
3.3.3.4.1.22	Node Lane Width	See 4.3.3.4.1.22, Node Lane Width	
3.3.3.4.1.23	Node Accuracy	See 4.3.3.4.1.23, Node Accuracy	
3.3.3.4.2	Lane Attributes		
3.3.3.4.2.1	Direction of Travel	See 4.3.3.4.2.1, Direction of Travel	
3.3.3.4.2.2	Lane Sharing	See 4.3.3.4.2.2, Lane Sharing	
3.3.3.4.2.3	Lane Type Attributes	See 4.3.3.4.2.3, Lane Type Attributes	
3.3.3.4.2.4	Lane Attributes - Vehicle	See 4.3.3.4.2.4, Lane Attributes - Vehicle	
3.3.3.4.2.5	Lane Attributes - Crosswalk	See 4.3.3.4.2.5, Lane Attributes - Crosswalk	
3.3.3.4.2.6	Lane Attributes - Bicycle	See 4.3.3.4.2.6, Lane Attributes - Bicycle	
3.3.3.4.2.7	Lane Attributes - Tracked Vehicles	See 4.3.3.4.2.7, Lane Attributes - Tracked Vehicles	
3.3.3.4.2.8	Lane Attributes - Parking	See 4.3.3.4.2.8, Lane Attributes - Parking	
3.3.3.4.3	Lane Maneuvers	See 4.3.3.4.3, Lane Maneuvers	
3.3.3.4.4	Connections Between Lanes		
3.3.3.4.4.1	Lane Connections	See 4.3.3.4.4.1, Lane Connections	
3.3.3.4.4.2	Connection Egress Lane	See 4.3.3.4.4.2, Connection Egress Lane	
3.3.3.4.4.3	Connection Maneuvers	See 4.3.3.4.4.3, Connection Maneuvers	
3.3.3.4.4.4	Connection Signal Group	See 4.3.3.4.4.4, Connection Signal Group	
3.3.3.4.4.5	Include Only Permitted Connections	See 4.3.3.4.4.5, Include Only Permitted Connections	
3.3.3.4.5	Speed Limit Information Requirements		
3.3.3.4.5.1	Default Speed Limit	See 4.3.3.4.5.1, Default Speed Limit	
3.3.3.4.5.2	Change in Lane Speed Limit	See 4.3.3.4.5.2, Change in Lane Speed Limit	
3.3.3.4.6	Revocable Lanes	See 4.3.3.4.6, Revocable Lanes	
3.3.3.4.7	MAP Message - Accuracy	No Further Design Details	
3.3.3.4.8	Signal Timing and Roadway Geometry Information Synchronization		
3.3.3.4.8.1	Matching Intersection Reference Identifier	No Further Design Details	
3.3.3.4.8.2	Matching SPaT and MAP Version	See 4.3.3.4.8.2, Matching SPaT and MAP Version	
3.3.3.5	Positioning Messages		
3.3.3.5.1	Positioning Corrections	See 4.3.3.5.1, Positioning Corrections	

Requirements Traceability Matrix (RTM)			
FR ID	Functional Requirement	Design Detail	Additional Specification
3.3.3.5.2	Real-Time Kinematics Requirements		
3.3.3.5.2.1	RSU Proximity	See 4.3.3.5.2.1, RSU Proximity	
3.3.3.5.2.2	Minimum RTCM Corrections Broadcast Frequency	No Further Design Details	
3.3.4	Security Requirements		
3.3.4.1	Connected Intersection System Trustworthiness Requirements		
3.3.4.1.1	SPaT Information Message Trustworthiness - RSU	See 4.3.4.1.1, SPaT Information Message Trustworthiness - RSU	
3.3.4.1.2	SPaT Information Message Trustworthiness - TSC Infrastructure	See 4.3.4.1.2, SPaT Information Message Trustworthiness - TSC Infrastructure	
3.3.4.1.3	MAP Data Trustworthiness	See 4.3.4.1.3, MAP Data Trustworthiness	
3.3.4.1.4	RTCM Corrections Data Trustworthiness	See 4.3.4.1.4, RTCM Corrections Data Trustworthiness	
3.3.4.2	Connected Intersection System Security Requirements		
3.3.4.2.1	Secure Network	See 4.3.4.2.1, Secure Network	
3.3.4.2.2	Assurance of Connection to Correct Network	See 4.3.4.2.2, Assurance of Connection to Correct Network	
3.3.4.3	Verification of Connected Intersection System Security Requirements		
3.3.4.3.1	Security Compliance Assessment	See 4.3.4.3.1, Security Compliance Assessment	
3.3.4.3.2	Point of Certification	See 4.3.4.3.2, Point of Certification	
3.3.4.4	Certificate Issuing Requirements		
3.3.4.4.1	Certificate Issuance	See 4.3.4.4.1, Certificate Issuance	
3.3.4.4.2	Certificate Nonissuance	See 4.3.4.4.2, Certificate Nonissuance	
3.3.4.4.3	CI Operation Security Practices	See 4.3.4.4.3, CI Operation Security Practices	
3.3.4.4.4	RSU Security Standards	See <i>RSU Standard v1.0</i> , Section 4.3.5.12 Secure Management of X.509 Credentials for TLS Design Details	
3.3.4.4.5	TSC Infrastructure Security Standards	See 4.3.4.4.5, TSC Infrastructure Security Standards	
3.3.4.5	Security Against Cyber Attack Requirements		

Requirements Traceability Matrix (RTM)			
FR ID	Functional Requirement	Design Detail	Additional Specification
3.3.4.5.1	Cyber-Attack Recovery Plan	See 4.3.4.5.1, Cyber-Attack Recovery Plan	
3.3.4.5.2	Cyber-Attack Robustness	See 4.3.4.5.2, Cyber-Attack Robustness	
3.3.4.5.3	Network Protection	See 4.3.4.5.3, Network Protection	
3.3.4.6	Data Flow: Communications and Interface Security Requirements		
3.3.4.6.1	Interface between RSU and TMS		
3.3.4.6.1.1	General RSU-TMS Interface Requirements		
3.3.4.6.1.1.1	Secure Transport of SNMPv3	See 4.3.4.6.1.1.1, Secure Transport of Use of SNMPv3	
3.3.4.6.1.1.2	Use of (D)TLS for Management Protocols	See 4.3.4.6.1.1.2, Use of (D)TLS for other Management Protocols	
3.3.4.6.1.1.3	Use of SSH	See 4.3.4.6.1.1.3, Use of SSH	
3.3.4.6.1.2	(D)TLS Certificate Requirements		
3.3.4.6.1.2.1	(D)TLS Authentication - Installation	See 4.3.4.6.1.2.1, (D)TLS Authentication - Installation	
3.3.4.6.1.2.2	(D)TLS Authentication - Rejection	See 4.3.4.6.1.2.2, (D)TLS Authentication - Rejection	
3.3.4.6.1.2.3	RSU Certificate Security	See 4.3.4.6.1.2.3, RSU Certificate Security	
3.3.4.6.1.2.4	RSU Client Certificate Security	See 4.3.4.6.1.2.4, RSU Client Certificate Security	
3.3.4.6.2	Interface between RSU and SCMS	See 4.3.4.6.2, Interface between RSU and SCMS	
3.3.4.6.3	Interface between an RSU and the OBU/MU	See 4.3.4.6.3, Interface between an RSU and the OBU/MU	
3.3.4.6.4	Interface between an RSU and the TSC Infrastructure		
3.3.4.6.4.1	Use of Secure Transport Protocol	See 4.3.4.6.4.1, Use of Secure Transport Protocol	
3.3.4.6.4.2	Use of TLS Protocol	See 4.3.4.6.4.2, Use of (D)TLS Protocol	
3.3.4.6.4.3	Protection against TSC Infrastructure Reconfiguration from the RSU	See 4.3.4.6.4.3, Protection against TSC Infrastructure Reconfiguration from the RSU	
3.3.4.6.4.4	Validation of Forwarded V2X Messages	See 4.3.4.6.4.4, Validation of Forwarded V2X Messages	
3.3.4.6.5	Interface between the TMS and the TSC Infrastructure	See 4.3.4.6.5, Interface between the TMS and the TSC Infrastructure	
3.3.4.6.6	Interface between the MAP Server and the TMS		
3.3.4.6.6.1	Secure Connection to MAP Server	See 4.3.4.6.6.1, Secure Connection to MAP Server	

Requirements Traceability Matrix (RTM)			
FR ID	Functional Requirement	Design Detail	Additional Specification
3.3.4.6.6.2	MAP Data Integrity	See 4.3.4.6.6.2, MAP Data Integrity	
3.3.4.6.6.3	MAP Data Signature	See 4.3.4.6.6.3, MAP Data Signature	
3.3.4.6.7	Interface between MAP Server and the SCMS	See 4.3.4.6.7, Interface between MAP Server and the SCMS	
3.3.4.7	Correct Operations Requirements		
3.3.4.7.1	Device Protection Requirements		
3.3.4.7.1.1	RSU Protection	See 4.3.4.7.1.1, RSU Protection	
3.3.4.7.1.2	Device Protection	See 4.3.4.7.1.2, Device Protection	
3.3.4.7.2	Secure Administration of RSU		
3.3.4.7.2.1	Secure RSU Administration User Interface	See <i>RSU Standard v1.0</i> , Section 4.3.5.11 Secure Administration Design	
3.3.4.7.2.2	Password Change Prompt	See 4.3.4.7.2.2, Password Change Prompt	
3.3.4.7.2.3	Remote Restart	See <i>RSU Standard v1.0</i> , Section 4.2.3 Requirements Traceability Matrix (RTM) Table, FR ID 3.3.2.1.2 RSU Restarts	
3.3.4.7.2.4	Log Restarts	See <i>RSU Standard v1.0</i> , Section 4.3.2.3 Log Restarts Design Details	
3.3.4.7.2.5	Factory Default	See <i>RSU Standard v1.0</i> , Section 4.3.2.2 Factory Default Design Details	
3.3.4.7.2.6	Protection against Tampering	See 4.3.4.7.2.6, Protection against Tampering	
3.3.4.7.2.7	Operational, Security and other Events Logging - RSU	See <i>RSU Standard v1.0</i> , Section 4.3.5.13 Logging for General and Security Purposes Design Details	
3.3.4.7.2.8	Operational Logging - TMS	See 4.3.4.7.2.8, Operational Logging - TMS	
3.3.4.7.2.9	Operational Logging - TSC Infrastructure	See 4.3.4.7.2.9, Operational Logging - TSC Infrastructure	
3.3.4.7.2.10	Determine Mode of Operations	See <i>RSU Standard v1.0</i> , Section 4.2.3 Requirements Traceability Matrix (RTM) Table, FR ID 3.3.3.2.1 Determine Mode of Operations.	
3.3.4.7.2.11	Determine Operational Status	See <i>RSU Standard v1.0</i> , Section 4.3.3.1 Monitor Current Status Design Details	
3.3.4.7.2.12	Determine Operational Performance	See <i>RSU Standard v1.0</i> , Section 4.2.3 Requirements Traceability Matrix (RTM) Table, FR ID 3.3.3.2.3 Determine Operational Performance	

Requirements Traceability Matrix (RTM)			
FR ID	Functional Requirement	Design Detail	Additional Specification
3.3.4.7.2.13	Determine Operating Environment	See <i>RSU Standard v1.0</i> , Section 4.2.3 Requirements Traceability Matrix (RTM) Table, FR ID 3.3.3.2.4 Determine Operating Environment	
3.3.4.7.2.14	Access Control Policy	See 4.3.4.7.2.14, Access Control Policy	
3.3.4.7.3	RSU Device Class Requirement	No Further Design Details	
3.3.4.7.4	TSC Device Class Requirement	No Further Design Details	
3.3.4.7.5	MAP Signer Device Class Requirement	No Further Design Details	
3.3.4.7.6	Authenticated Secure Update Requirements		
3.3.4.7.6.1	RSU Software and Firmware Updates	See 4.3.4.7.6.1, RSU Software and Firmware Updates	
3.3.4.7.6.2	Trustworthiness of Software and Firmware Updates	See 4.3.4.7.6.2, Trustworthiness of Software and Firmware Updates	
3.3.4.7.6.3	TSC Infrastructure Software and Firmware Updates	See 4.3.4.7.6.3, TSC Infrastructure Software and Firmware Updates	
3.3.4.8	Network Monitoring Requirements	See 4.3.4.8, Network Monitoring Design	
3.3.4.9	Credential Management Requirements		
3.3.4.9.1	Credential Provisioning – (D)TLS Requirements		
3.3.4.9.1.1	Start-up Initialization	See 4.3.4.9.1.1, Start-up Initialization	
3.3.4.9.1.2	Credential Updates	See 4.3.4.9.1.2, Credential Updates	
3.3.4.9.2	Management of Untrustworthy Devices - TLS Requirements		
3.3.4.9.2.1	Monitor Certificate Status	See 4.3.4.9.2.1, Monitor Certificate Status	
3.3.4.9.2.2	Drop Connections	See 4.3.4.9.2.2, Drop Connections	
3.3.4.9.3	Credential System Access - SCMS Requirements		
3.3.4.9.3.1	Connectivity Requirement	See 4.3.4.9.3.1, Connectivity Design	
3.3.4.9.3.2	Download SCMS Files	See 4.3.4.9.3.2, Download SCMS Files	

4.3 Design Details

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

4.3.1 Architectural Design Details

The design details to fulfill the architectural requirements defined in Section 3.3.1 follow.

4.3.1.1 IEEE Std 802.11-2016 (DSRC)

No design details provided at this time.

4.3.1.2 3GPP PC5 Mode 4 (Release 14 or 15 (C-V2X))

No design details provided at this time.

4.3.2 TSC Infrastructure to RSU Design Details

The design details to fulfill the requirements for a TSC infrastructure to provide signal timing information to an RSU follow. These requirements are defined in Section 3.3.2.

4.3.2.1 TSC Infrastructure Signal Timing Data Design Details

The design details to fulfill the requirements for a TSC infrastructure to provide signal phase and timing data to an RSU follow. These requirements are defined in Section 3.3.2.1.

4.3.2.1.1 SPaT Information Messages Design Details

This design details to fulfill the requirements defined in Section 3.3.2.1.1 follow.

The SAE J2735_202007 SPaT message transmitted by a connected intersection uses SPaT information sent from the TSC infrastructure to the RSU, and is called the SPaT information message in this document (See Figure 14). Three formats in which SPaT information may be sent to the RSU are the following:

- Using the *NTCIP 1202 v03A* Standard;
- Using the *V2I Hub Interface Control Document (V2I Hub ICD)* Traffic Signal Controller Broadcast Message (TSCBM); and
- Using the MSG_SignalPhaseAndTiming Message (SPaT) message defined in *SAE J2735_202007*.

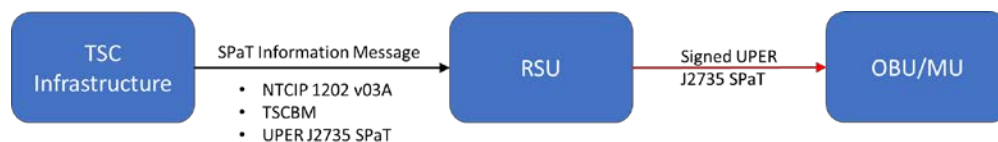


Figure 14. SPaT Information Message

4.3.2.1.1.1 NTCIP 1202A v03 SPaT Information

The design details to use NTCIP 1202 v03A to transmit a SPaT information message are as follows.

NTCIP 1202 v03A defines data objects that provide the information needed by an RSU to generate a UPER-encoded SPaT message. The requirements for generating the SPaT message can be found in Section 3.5.4 of *NTCIP 1202 v03A*. The design details to fulfill each of those requirements are found in the Requirements Traceability Matrix for *NTCIP 1202 v03A*, which is found in Annex A.3.

The RSU then uses this information to generate a UPER-encoded SAE J2735_202007 SPaT message.

Notes:

- A connected intersection uses UTC time (See 3.3.3.2.1, Time Accuracy), however not all TSC infrastructure uses UTC time. Thus, an RSU must convert the timepoints (or ticks) provided by the TSC infrastructure into UTC time to properly generate a SPaT message.

4.3.2.1.1.2 TSCBM SPaT Information

The design details to transmit a SPaT information message using the TSCBM is described in the section titled Traffic Signal Controller Interface in Chapter 3 of the *V2I Hub Interface Control Document (ICD)*. This section describes the data objects that have to be exchanged between the TSC infrastructure and the RSU. The data objects consist of NTCIP 1202 v02 data objects, as described in Table 3-2, *NTCIP 1202 v03A Interface SNMP Data Objects*, of the ICD; and additional data objects, listed in Table 3-3, *Extended SNMP Data Objects*, of the ICD. The additional, or extended, data objects along with several NTCIP data objects are sent in a single message, also known as the Traffic Signal Controller Broadcast Message (TSCBM). The structure of the TSCBM is described in Table 3-4 of the ICD.

The RSU then uses this information to generate a UPER-encoded SAE J2735_202007 SPaT message.

Notes:

- Times provided in the TSCBM are time to change, unlike the SAE J2735_202007 SPaT message, which provides the time mark (time of change) when a signal indication will change. Thus, an RSU must convert the time to change information into a time mark to properly generate a SPaT message.
- The TSCBM does not assign a signal group ID. Thus, an RSU has to have a translation table to convert the phases/overlaps to a signal group ID to generate a SPaT message.
- The TSCBM does not indicate if a movement/phase is a protected or permissive movement. Thus, an RSU has to have a table to indicate if a phase/overlap is a protected or permissive movement/clearance.
- Some information required for the SPaT information is not provided by the TSC infrastructure and must be provided by the RSU, such as intersection ID and enabled Lanes.
- The RSU may have to convert the spatTimestamp in the TSCBM into UTC time. The spatTimestamp may be based on the clock that the controller is using, which may be different than UTC time.

4.3.2.1.1.3 SPaT Message

Some TSC infrastructure systems are capable of generating a UPER-encoded SAE J2735_202007 SPaT message directly. If the TSC infrastructure system can generate a complete UPER-encoded SAE J2735_202007 SPaT message, the TSC infrastructure system should transmit the SPaT message to the RSU and store it in the Immediate Forward Message (IFM) table of the RSU.

The IFM table is called rsulFMStatusTable if the RSU complies with the RSU Specification v4.1, and is also called the rsulFMStatusTable in *NTCIP 1218 v01*, or the proposed *RSU Standard v1.0*, which references NTCIP 1218 v01. Note that although the IFM table has the same name in the RSU Specification v4.1 MIB and NTCIP 1218 v01, the contents of the tables are different.

If the RSU is using NTCIP 1218 v01, upon receiving the UPER-encoded SPaT message, the appropriate entry in the IFM table will determine what security processing is to be performed before the SPaT message is broadcasted.

4.3.2.1.2 TSC SPaT Information Message Transmission Rate

No design details provided at this time.

4.3.2.1.3 TSC SPaT Information Message Transmission Rate Tolerance

No design details provided at this time.

4.3.2.1.4 TSC SPaT Information Message Update Latency

No design details provided at this time.

4.3.2.1.5 TSC Infrastructure Processing Latency

No design details provided at this time.

4.3.2.2 Signal Timing Status Design Details

The design details to fulfill the requirements for a TSC infrastructure to provide signal timing status to an RSU follow. These requirements are defined in Section 3.3.2.2.

4.3.2.2.1 TSC Infrastructure Manual Control Indication Design Detail

The design for the TSC infrastructure Manual Control Indication depends on what format is used to exchange SPaT information from the TSC infrastructure to the RSU. Also see Annex A.2.1.9, Manual Control.

4.3.2.2.1.1 TSC Infrastructure Manual Control Indication (NTCIP 1202 v03A)

When sending NTCIP 1202 v03A data, NTCIP Object spatStatus Bit 0 is enabled (1) when NTCIP Object unitControlStatus is set to remoteManualControl (9) or localManualControl (10). Otherwise, NTCIP Object spatStatus Bit 0 is disabled (0).

4.3.2.2.1.2 TSC Infrastructure Manual Control Indication (TSCBM)

When sending TSCBMs, TSCBM Byte 232 Bit 0 is set to 1 when NTCIP Object unitControlStatus is set to remoteManualControl (9) or localManualControl (10). Otherwise, TSCBM Byte 232 Bit 0 is set to 0.

4.3.2.2.1.3 TSC Infrastructure Manual Control Indication (SAE J2735)

When sending SAE J2735_202007 SPaT messages, DE_IntersectionStatusObject Bit 0 is set to 1 when NTCIP Object unitControlStatus is set to remoteManualControl (9) or localManualControl (10). Otherwise, DE_IntersectionStatusObject Bit 0 is set to 0. Also see Section 4.3.3.3.2.1.

4.3.2.2.2 TSC Infrastructure Stop Time Indication

The design for the TSC Infrastructure Stop Time Indication depends on what format is used to exchange SPaT information from the TSC infrastructure to the RSU. Also see Annex A.2.1.8, Stop Time.

4.3.2.2.2.1 TSC Infrastructure Stop Time Indication (NTCIP 1202 v03A)

When sending NTCIP 1202 v03A data, NTCIP Object spatStatus Bit 1 is enabled (1) when NTCIP Object unitAlarmStatus2 Bit 4 is True (1). Otherwise, NTCIP Object spatStatus Bit 1 is disabled (0).

4.3.2.2.2 TSC Infrastructure Stop Time Indication (TSCBM)

When sending TSCBMs, TSCBM Byte 232 Bit 1 is set to 1 when NTCIP Object unitAlarmStatus2 Bit 4 is True (1). Otherwise, TSCBM Byte 232 Bit 1 is set to 0.

4.3.2.2.3 TSC Infrastructure Stop Time Indication (SAE J2735)

When sending SAE J2735_202007 SPaT messages, DE_IntersectionStatusObject Bit 1 is set to 1 when NTCIP Object unitAlarmStatus2 Bit 4 is True (1). Otherwise, DE_IntersectionStatusObject Bit 1 is set to 0. Also see Section 4.3.3.2.2.

4.3.2.2.3 TSC Infrastructure Cabinet Flash (Exception Flash) Indication

The design for the TSC Infrastructure Cabinet Flash (Exception Flash) Indication depends on what format is used to exchange SPaT information from the TSC infrastructure to the RSU. Also see 4.3.3.2.3, Failure Flash; Annex A.2.1.6, Hard Flashing Operation; and A.2.1.7, Tech Flash.

Cabinet Flash is any type of flash that is initiated and terminated by sources external to the controller. There are two types of Cabinet Flash:

- “Monitor Flash” is Cabinet Flash controlled by the monitor in the following two scenarios:
 - When resuming operation after a power loss or interruption, the monitor keeps the Flash Bus energized for a minimum of 6 seconds before energizing the Signal Bus and transferring control to the controller.
 - When a fault is detected by the monitor, it energizes the Flash Bus until either the fault is cleared by pressing the Reset button on the monitor (latching fault) or, with certain types of faults, when the condition that caused the fault is no longer present (non-latching fault).
- “Local Flash” is Cabinet Flash controlled by human-operated switches in the cabinet, typically labeled “AUTO/FLASH,” that are used by technicians to flash the signals when performing maintenance on the controller (Tech Flash) or by police during unusual traffic conditions or situations (Police Flash).

The end of Cabinet Flash is indeterminate because the controller does not know when the monitor is going to be reset or when the flash switch is going to be moved from “FLASH” to “AUTO.” Therefore, time change details during Cabinet Flash cannot be supplied.

During Cabinet Flash, signal indications are determined by cabinet wiring (jumpers or flash program blocks) rather than controller software, so the controller does not have intrinsic knowledge of the signal indications during Cabinet Flash. A workaround for this may be provided in future versions of this document, perhaps using new NTCIP objects (per-channel entry of Yellow, Red, or Dark to match physical wiring) or real-time voltage and current measurements (where supported by serial cabinet architectures).

Certain cabinet architectures such as NEMA TS 1 do not define Flash Sense inputs to the controller. IOOs using these cabinets are cautioned that, without special accommodations, controllers running in these cabinets do not know that Cabinet Flash is active and may continue to cycle normally and erroneously provide normal time change details and movement phase states to OBUs/MUs during Cabinet Flash.

4.3.2.2.3.1 TSC Infrastructure Cabinet Flash (Exception Flash) Indication (NTCIP 1202 v03A)

When sending NTCIP 1202 v03A data, NTCIP Object spatStatus Bit 2 is enabled (1) when NTCIP Object unitFlashStatus is other (1), localManual (4), or mmu (6). Otherwise, NTCIP Object spatStatus Bit 2 is disabled (0).

TSC Infrastructure can be in either Cabinet Flash or Controller Flash, but not both. Therefore, NTCIP Object spatStatus Bit 2 and Bit 7 shall not simultaneously equal 1.

4.3.2.2.3.2 TSC Infrastructure Cabinet Flash (Exception Flash) Indication (TSCBM)

When sending TSCBM, TSCBM Byte 232 Bit 2 is set to 1 when NTCIP Object unitFlashStatus is other (1), localManual (4), or mmu (6). Otherwise, TSCBM Byte 232 Bit 2 is set to 0.

TSC Infrastructure can be in either Cabinet Flash or Controller Flash, but not both. Therefore, TSCBM Byte 232 Bit 2 and Bit 7 shall not simultaneously equal 1.

4.3.2.2.3.3 TSC Infrastructure Cabinet Flash (Exception Flash) Indication (SAE J2735)

When sending SAE J2735_202007 SPaT messages, DE_IntersectionStatusObject Bit 2 is set to 1 when NTCIP Object unitFlashStatus Bit 2 is enabled (1) when NTCIP Object unitFlashStatus is other (1), localManual (4), or mmu (6). Otherwise, DE_IntersectionStatusObject Bit 2 is set to 0. Also see Section 4.3.3.3.2.8.

TSC Infrastructure can be in either Cabinet Flash or Controller Flash, but not both. Therefore, DE_IntersectionStatusObject Bit 2 and Bit 7 shall not simultaneously equal 1.

4.3.2.2.4 TSC Infrastructure Controller Flash (Operational Flash) Indication

The design for the TSC Infrastructure Controller Flash (Operational Flash) Indication depends on what format is used to exchange SPaT information from the TSC infrastructure to the RSU. Also see 4.3.3.3.2.8, Standby Mode; and Annex A.2.1.5, Soft Flashing Operation.

Controller Flash is any type of flash that is initiated and terminated by the controller. The controller enters and exits Controller Flash in a controlled, deterministic manner and, as such, shall provide time change details for flash entry and flash exit intervals. The time change details that shall be provided differs by Controller Flash type, of which there are four:

- “Startup Flash” is a transitory interval timed immediately after the monitor transfers control to the controller. The duration of Startup Flash is controlled by the NTCIP unitStartupFlash object, which may be 0. The following time change intervals are deterministic during Startup Flash:
 - Minimum End Time: use NTCIP 1202 v03A unitStartupFlash
- “Automatic Flash” is commanded by NTCIP Pattern 255, either manually or on a scheduled basis. It is typically used as an operational strategy during off-peak or overnight times when steady (stop-and-go) operation is not warranted. The following time change intervals may be deterministic during Scheduled Flash:
 - Maximum End Time: use NTCIP 1202 v03A schedules (TOD schedule look ahead is optional per A.2.1.1)
- “Preempt Flash” occurs during a preempt’s Dwell state if the preempt’s NTCIP preemptControl Bit 3 (Flash Dwell) = 1; the following time change details may be deterministic during Preempt Flash:
 - Minimum End Time: use NTCIP 1202 v03A preemptDwellGreen
 - Maximum End Time: use NTCIP 1202 v03A preemptMaximumPresence
- “Fault Monitor Flash” occurs when the controller detects an anomaly in the TSC Infrastructure, such as a mismatch between its copy of the permissive channels and the monitor’s copy of the permissive channels. The way the controller causes Fault Monitor Flash differs by cabinet architecture. For example, the controller sets the Fault Monitor output to FALSE in NEMA TS 2 Type 1 cabinets and sets Message Type 62 Bit 1 to 1 in ITS and ATC cabinets. The controller exits Fault Monitor Flash when the anomaly is no longer present. Contrast Fault Monitor Flash with Fault Flash, which is initiated by the monitor and persists until the monitor is reset. The controller sets NTCIP unitFlashStatus to 3 (faultMonitor) during Fault Monitor Flash.

When Controller Flash is performed through the Signal Bus (load switches or switch packs), the signal indications (flashing red, yellow, or not at all/dark) are controlled by the controller, so the controller shall

report the movement phase states. However, when Controller Flash is performed through the Flash Bus due to either controller software behavior (for example, by setting the Fault Monitor output to FALSE) or if the cabinet is specially wired (e.g., connecting a Flash output from the controller to the cabinet's Main Contactor), signal indications are determined by cabinet wiring (jumpers or flash program blocks) rather than controller software and the controller does not have intrinsic knowledge of the signal indications. Therefore, the controller shall set movement phase states to Unavailable during Controller Flash performed through the Flash Bus. A workaround for this may be provided in future versions of this document, perhaps using new NTCIP objects (per-channel entry of Yellow, Red, or Dark to match physical wiring) or real-time voltage and current measurements (where supported by serial cabinet architectures).

4.3.2.2.4.1 TSC Infrastructure Controller Flash (Operational Flash) Indication (NTCIP 1202 v03A)

When sending NTCIP 1202 v03A data, NTCIP Object spatStatus Bit 7 is enabled (1) when NTCIP Object unitFlashStatus is automatic (3), faultMonitor (5), startup (7), or preempt (8). Otherwise, NTCIP Object spatStatus Bit 7 is disabled (0).

If Controller Flash is performed through the Flash Bus, NTCIP signalState = unavailable (0) for every channel and movement.

TSC Infrastructure can be in either Cabinet Flash or Controller Flash, but not both. Therefore, NTCIP Object spatStatus Bit 2 and Bit 7 shall not simultaneously equal 1.

4.3.2.2.4.2 TSC Infrastructure Controller Flash (Operational Flash) Indication (TSCBM)

When sending TSCBMs, TSCBM Byte 232 Bit 7 is set to 1 when NTCIP Object unitFlashStatus is automatic (3), faultMonitor (5), startup (7), or preempt (8). Otherwise, TSCBM Byte 232 Bit 7 is set to 0.

If Controller Flash is performed through the Flash Bus, TSCBM Bytes 210–231 = zero (0).

TSC Infrastructure can be in either Cabinet Flash or Controller Flash, but not both. Therefore, TSCBM Byte 232 Bit 2 and Bit 7 shall not simultaneously equal 1.

4.3.2.2.4.3 TSC Infrastructure Controller Flash (Operational Flash) Indication (SAE J2735)

When sending SAE J2735_202007 SPaT messages, DE_IntersectionStatusObject Bit 7 is set to 1 when NTCIP Object unitFlashStatus is automatic (3), faultMonitor (5), startup (7), or preempt (8). Otherwise, DE_IntersectionStatusObject Bit 7 is set to 0. Also see Section 4.3.3.3.2.7, Traffic Dependent Mode.

If Controller Flash is performed through the Flash Bus, SPaT MovementPhaseState = unavailable (0) for every movement.

TSC Infrastructure can be in either Cabinet Flash or Controller Flash, but not both. Therefore, DE_IntersectionStatusObject Bit 2 and Bit 7 shall not simultaneously equal 1.

4.3.2.2.5 TSC Infrastructure Preemption Operation Indication

The design for the TSC Infrastructure Preemption Operation Indication depends on what format is used to exchange SPaT information from the TSC infrastructure to the RSU.

4.3.2.2.5.1 TSC Infrastructure Preemption Operation Indication (NTCIP 1202 v03A)

When sending NTCIP 1202 v03A data, NTCIP Object spatStatus Bit 3 is enabled (1) when NTCIP Object preemptState is any value other than other (1), notActive (2), or notActiveWithCall (3). Otherwise, NTCIP Object spatStatus Bit 3 is disabled (0).

4.3.2.2.5.2 TSC Infrastructure Preemption Operation Indication (TSCBM)

When sending TSCBMs, TSCBM Byte 232 Bit 3 is set to 1 when NTCIP Object preemptState is any value other than other (1), notActive (2), or notActiveWithCall (3). Otherwise, TSCBM Byte 232 Bit 3 is set to 0.

4.3.2.2.5.3 TSC Infrastructure Preemption Operation Indication (SAE J2735)

When sending SAE J2735_202007 SPaT messages, DE_IntersectionStatusObject Bit 3 is set to 1 when NTCIP Object preemptState is any value other than other (1), notActive (2), or notActiveWithCall (3). Otherwise, DE_IntersectionStatusObject Bit 3 is set to 0. Also see Section 4.3.3.3.2.4.

4.3.2.2.6 TSC Infrastructure Priority Operation Indication

The design for the TSC Infrastructure Priority Operation Indication depends on what format is used to exchange SPaT information from the TSC infrastructure to the RSU.

4.3.2.2.6.1 TSC Infrastructure Priority Operation Indication (NTCIP 1202 v03A)

When sending NTCIP 1202 v03A data, NTCIP Object spatStatus Bit 4 is enabled (1) when the TSC infrastructure is servicing a priority request. This does not include any time to transition. Otherwise, NTCIP Object spatStatus Bit 4 is disabled (0).

The purpose here is to indicate to OBU/MUs when TSC infrastructure timing might be affected. If a request for service can be fulfilled without changes to the current signal timing, then this bit would remain disabled.

4.3.2.2.6.2 TSC Infrastructure Priority Operation Indication (TSCBM)

When sending TSCBMs, TSCBM Byte 232 Bit 4 is set to 1 when the TSC infrastructure is servicing a priority request. Otherwise, TSCBM Byte 232 Bit 4 is set to 0.

4.3.2.2.6.3 TSC Infrastructure Priority Operation Indication (SAE J2735)

When sending SAE J2735_202007 SPaT messages, DE_IntersectionStatusObject Bit 4 is set to 1 when the TSC infrastructure is servicing a priority request. This does not include any time to transition. Otherwise, DE_IntersectionStatusObject Bit 4 is set to 0. See also Section 4.3.3.3.2.5.

The purpose here is to indicate to OBU/MUs when TSC timing might be affected. If a request for service can be fulfilled without changes to the current signal timing then this bit would remain 0.

4.3.2.2.7 TSC Infrastructure Fixed Time Control Indication

The design for the TSC Infrastructure Fixed Time Control Indication depends on what format is used to exchange SPaT information from the TSC infrastructure to the RSU.

4.3.2.2.7.1 TSC Infrastructure Fixed Time Indication (NTCIP 1202 v03A)

When sending NTCIP 1202 v03A data, NTCIP Object spatStatus Bit 5 is enabled (1) when the TSC infrastructure is operating in fixed time control. Otherwise, NTCIP Object spatStatus Bit 5 is disabled (0).

One of NTCIP Object spatStatus Bit 5 and Bit 6 is always enabled and the bits are mutually exclusive.

NTCIP Object spatStatus Bit 5 and Bit 6 represent the general programming of the TSC infrastructure. These bits are not dynamic changing cycle by cycle or by a preemption operation.

4.3.2.2.7.2 TSC Infrastructure Fixed Time Indication (TSCBM)

There is no TSCBM element for a fixed time indication.

4.3.2.2.7.3 TSC Infrastructure Fixed Time Indication (SAE J2735)

When sending SAE J2735_202007 SPaT messages, DE_IntersectionStatusObject Bit 5 is set to 1 when the TSC infrastructure is operating in fixed time control. Otherwise, DE_IntersectionStatusObject Bit 1 is set to 0. See also Section 4.3.3.3.2.6.

One of DE_IntersectionStatusObject Bit 5 and Bit 6 is always 1 and the bits are mutually exclusive.

DE_IntersectionStatusObject Bit 5 and Bit 6 represent the general programming of the TSC infrastructure. These bits are not dynamic changing cycle by cycle or by a preemption operation.

4.3.2.2.8 TSC Infrastructure Non-Fixed Time Control

The design for the TSC Infrastructure Non-Fixed Time Control Indication depends on what format is used to exchange SPaT information from the TSC infrastructure to the RSU. Non-fixed time control is called trafficDependentOperation in the SAE J2735_202007 SPaT message. Semi-actuated control, which is a legacy term, is considered non-fixed time.

4.3.2.2.8.1 TSC Infrastructure Non-Fixed Time Indication (NTCIP 1202 v03A)

When sending NTCIP 1202 v03A data, NTCIP Object spatStatus Bit 6 is enabled (1) when the TSC infrastructure is operating in non-fixed time control. Otherwise, NTCIP Object spatStatus Bit 6 is disabled (0).

One of NTCIP Object spatStatus Bit 5 and Bit 6 is always enabled and the bits are mutually exclusive.

NTCIP Object spatStatus Bit 5 and Bit 6 represent the general programming of the TSC infrastructure. These bits are not dynamic changing cycle by cycle or by a preemption operation.

4.3.2.2.8.2 TSC Infrastructure Non-Fixed Time Indication (TSCBM)

There is no TSCBM element for a non-fixed time indication.

4.3.2.2.8.3 TSC Infrastructure Non-Fixed Time Indication (SAE J2735)

When sending SAE J2735_202007 SPaT messages, DE_IntersectionStatusObject Bit 6 is set to 1 when the TSC infrastructure is operating in non-fixed time control. Otherwise, DE_IntersectionStatusObject Bit 6 is set to 0. See also Section 4.3.3.3.2.7.

One of DE_IntersectionStatusObject Bit 5 and Bit 6 is always 1 and the bits are mutually exclusive.

4.3.2.3 TSC Infrastructure RLVW Design Details

The design details to fulfill the requirements for a TSC infrastructure to provide support for the RLVW application follow. These requirements are defined in Section 3.3.2.3. The scenario describing the operation is in Section 2.6.1.

4.3.2.3.1 TSC Infrastructure Assured Green End Time (AGET) Design

The design details to provide an AGET follow.

4.3.2.3.1.1 TSC Infrastructure AGET (NTCIP 1202 v03A)

When sending NTCIP 1202 v03A data, if the TSC infrastructure has determined a specific termination time for a green signal indication for a channel representing a through traffic movement, the TSC infrastructure shall set the NTCIP SignalStatusEntry objects signalStateMinEndTick and signalStateMaxEndTick for the channel to the termination time. The termination time shall be equal to or greater than the original signalStateMinEndTick.

Note: Signal status information is arranged by channels in *NTCIP 1202 v03A*.

4.3.2.3.1.2 TSC Infrastructure AGET (TSCBM)

When sending TSCBMs, if the TSC infrastructure has determined a specific termination time for a green signal indication for a channel representing a through traffic movement, the TSC infrastructure shall set the TSCBM elements spatVehMinTimeToChange and spatVehMaxTimeToChange for the associated phase to the duration of time until the termination time. This duration shall be equal to or greater than the original spatVehMinTimeToChange.

Note: The TSCBM provides signal indication end times organized by phases in Bytes 2-209 and provides time-to-change values instead of the time-of-change values used by NTCIP 1202 v03A and SAE J2735_202007 SPaT messages. The RSU is required to convert these to time-of-change.

4.3.2.3.1.3 TSC Infrastructure AGET (SAE J2735)

When sending SAE J2735_202007 SPaT messages, if the TSC infrastructure has determined a specific termination time for a green signal indication for a channel representing a through traffic movement, the TSC infrastructure shall set the SAE J2735_202007 DF_TimeChangeDetails elements MinEndTime and MaxEndTime for the movement to the termination time. The termination time shall be equal to or greater than the original MinEndTime.

Note: Time change details are arranged by movements in *SAE J2735_202007*.

4.3.2.3.2 TSC Infrastructure Assured Green Period (AGP) Design Details

The AGP is calculated based on the following design.

The section provides the calculations for the design elements used by the TSC infrastructure to support the RLVW application. All values used to calculate the Assured Green Period, such as the yellow and red change interval durations, should be based using engineering practices such as ITE's *Traffic Control Devices Handbook* and in ITE's *Manual of Traffic Signal Design*. Annex B contains examples of using the calculations.

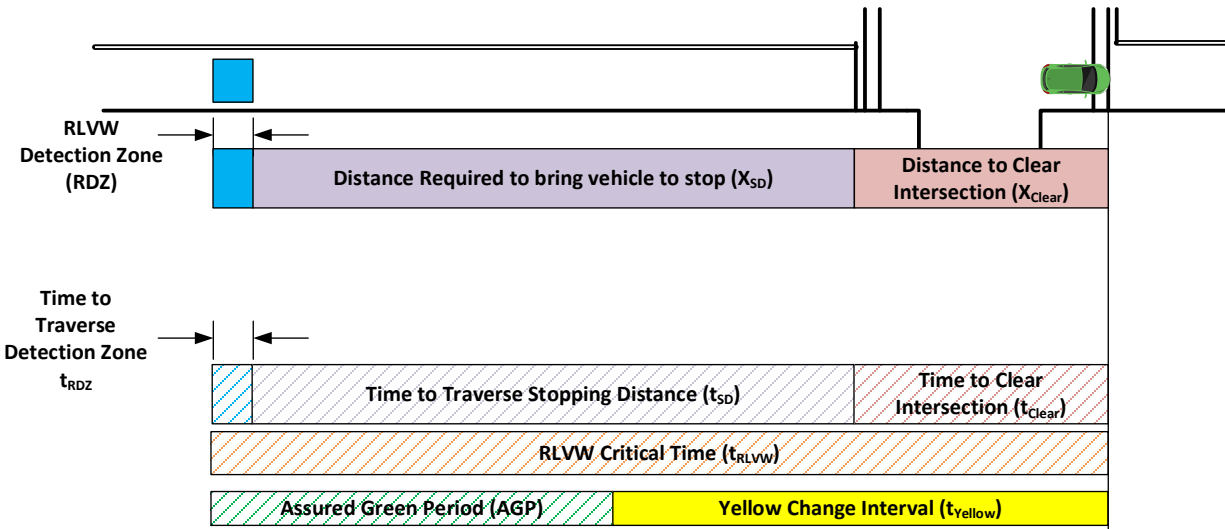


Figure 15. Distance and Time Elements of the TSC Infrastructure RLVW Design.

Variables and constants used in the RLVW calculations are as follows:

- $V_{Approach}$ is the approach speed of the vehicle which is the 85th percentile speed or the posted speed plus 7 mph converted to: a) feet per second (f/s) by multiplying by 1.47 or b) meters per second (m/s) by multiplying by 0.447
- **RDZ** is the RLVW Detection Zone which has a width equal to that of the lane and a length equal to time to detect vehicles (t_{RDZ}) multiplied by the approach speed
- X_{SD} is the distance required to bring the vehicle to a stop
- X_{Clear} is the distance to clear the intersection
- t_{RDZ} is the time required to traverse the RDZ at the approach speed (0.5 seconds is used to assure that at least one BSM message from an OBU/MU will be received by the TSC)
- t_{SD} is the time to traverse the stopping distance
- t_{Clear} is the time to traverse the clear distance to clear the intersection
- t_{RLVW} is the RLVW Critical Time which is the total time to be used by the RLVW application
- t_{Yellow} is the duration of the yellow change interval
- $t_{P/R}$ is the perception/reaction time (1.0 second is used)
- **G** is the acceleration due to gravity which is 32.2 f/s² or 9.81 m/s²
- **g** is the grade which is feet per feet (assumed level) where g is positive for an uphill grade approaching the signal, which allows faster deceleration
- **a** is ITE's deceleration constant of 10 ft/s² or 3.01 m/s²

The RLVW calculations are as follows:

- a) Length of the RLVW Detection Zone (RDZ)

$$RDZ = t_{RDZ} * V_{Approach}$$

- b) Stopping Distance (Basic Kinematic Equation)

$$X_{SD} = V_{Approach} t_{P/R} + \frac{V_{Approach}^2}{2(a \pm Gg)}$$

- c) Time to Clear Intersection at Approach Speed

$$t_{Clear} = \frac{X_{Clear}}{V_{Approach}}$$

- d) Time to Travel Through Stopping Distance at Approach Speed

$$t_{SD} = \frac{X_{SD}}{V_{Approach}}$$

- e) Red Light Violation Warning Critical Time

$$t_{RLVW} = t_{SD} + t_{Clear} + t_{RDZ}$$

- f) Assured Green Period (AGP)

$$AGP = t_{RLVW} - t_{Yellow}$$

4.3.2.3.3 TSC Infrastructure Minimum End Time with AGP Design Details

The design details to provide an increase in the minimum end time by the AGP follow.

NOTE: It is assumed that the TSC infrastructure will actually use the minimum end time by the AGP.

4.3.2.3.3.1 TSC Infrastructure Minimum End Time with AGP (NTCIP 1202 v03A)

When sending NTCIP 1202 v03A data, check the MAP message for signal groups that are identified as through movements then check the associated channels in NTCIP Object channelStatusGroupGreens to determine if the signal is green. If the signal is green, a vehicle is detected in the associated RDZ, and an AGET has not been set; then the TSC infrastructure shall set the NTCIP SignalStatusEntry object signalStateMinEndTick for the channel to the current time plus the AGP, unless the signalStateMinEndTick is already greater than the AGP. The signalStateMinEndTick shall never exceed the maximum green time for the phase.

Note: Signal status information is arranged by channels in NTCIP 1202 v03A.

4.3.2.3.3.2 TSC Infrastructure Minimum End Time with AGP (TSCBM)

When sending TSCBMs, check the MAP message for signal groups that are identified as through movements then check the associated channels in NTCIP Object channelStatusGroupGreens to determine if the signal is green. If the signal is green, a vehicle is detected in the associated RDZ, and an AGET has not been set, then the TSC infrastructure shall set the TSCBM element spatVehMinTimeToChange for the phase to the duration of the previous spatVehMinTimeToChange plus the AGP, unless the spatVehMinTimeToChange is already greater than the AGP. The spatVehMinTimeToChange shall never exceed the maximum green time for the phase.

Note: The TSCBM provides signal indication end times organized by phases in Bytes 2-209 and provides time-to-change values (durations in tenths of a second) instead of the time-of-change values used by NTCIP 1202 v03A and SAE J2735_202007 SPaT messages.

4.3.2.3.3.3 TSC Infrastructure Minimum End Time with AGP (SAE J2735)

When sending SAE J2735_202007 SPaT messages, check the MAP message for signal groups that are identified as through movements then check the associated channels in NTCIP Object

channelStatusGroupGreens to determine if the signal is green. If a signal is green, a vehicle is detected in the associated RDZ, and an AGET has not been set, then the TSC infrastructure shall set *the SAE J2735_202007 DF_TimeChangeDetails* element MinEndTime for the movement to the current time plus the AGP, unless the minEndTime is already greater than the AGP. The minEndTime shall never exceed the maximum green time for the phase.

Note: Time change details are arranged by movements in *SAE J2735_202007*.

4.3.3 Message Design Details

The design details to fulfill the requirements for a connected intersection broadcasting messages to OBUs/MUs follow. These requirements are defined in Section 3.3.3.

4.3.3.1 Message Performance Design Details

The design details to fulfill the performance requirements for a connected intersection broadcasting messages to OBUs/MUs follow. These requirements are defined in Section 3.3.3.1.

4.3.3.1.1 Uniform Message Design Details

The design details to fulfill requirements to provide a consistent representation of the situation and operating conditions at a connected intersection follow. These requirements are defined in Section 3.3.3.1.1.

4.3.3.1.1.1 SPaT Message - SAE J2735 Design Details

See MSG_SignalPhaseAndTiming Message (SPaT) in *SAE J2735_202007*.

NOTE: This CI Implementation Guide references *SAE J2735_202007*. At the time of publication, most implementations use the *SAE J2735_201603* version. There are some differences between the March 2016 version and the July 2020 version - implementers should be aware of the changes, such as the change in definition for DE_TimeMark.

4.3.3.1.1.2 SPaT Message - Mandatory Data Elements Design Details

See MSG_SignalPhaseAndTiming Message (SPaT) in *SAE J2735_202007*.

4.3.3.1.1.3 SPaT Message - CI Mandatory Data Element Design Details

Table 7 lists the data frames (begins with DF_) and the data elements (begins with DE_) in the MSG_SignalPhaseAndTiming Message (SPaT) message of *SAE J2735_202007* that are mandatory to be supported by a connected intersection to conform to the CI Implementation Guide. The data frames and data elements are listed in the order it appears in the SPaT message. Note that all data frames and data elements listed in Table 7 shall be supported by a connected intersection, however, several data frames and data elements do not have to be included in every broadcasted message under certain conditions.

The "SAE J2735 Mandatory" column indicates if the data frame or data element is mandatory to describe signal phase and timing data as defined in *SAE J2735_202007*. A value of M indicates that the data frame or data element is mandatory, while a value of O indicates that the data frame or data element is optional.

The "CI Implementation" column indicates if the data frame or data element is mandatory to be included in every broadcast SPaT message as defined by the CI Implementation Guide. A value of M indicates the data frame or data element must be included in every SPaT message broadcasted. A value of C indicates the data frame or data element is conditionally mandatory, meaning that the data frame or data element

shall be broadcasted if certain conditions are met. Those conditions can be found in the referenced section in parentheses.

For example, if there are no revocable lanes associated with an intersection, the data frame DF_EnabledLaneList is never transmitted in the SPaT message for that intersection. However, if a revocable lane is associated with that intersection (as defined in the MAP message for that intersection) and the revocable lane is active ("enabled"), then the data frame DF_EnabledLaneList shall be included in the SPaT message. These conditions are found in Section 4.3.3.3.7.

Similarly, if the TSC infrastructure provides a startTime for a signalGroupID, then startTime (DE_TimeMark) shall be included in the SPaT message. If the TSC infrastructure does not provide a startTime for a signalGroup, then startTime (DE_TimeMark) is not included in the SPaT message. These conditions are found in Sections 4.3.3.3.5.7 and 4.3.3.3.5.8.

Table 7. SPaT Message - Required Elements

SAE J2735 Data Frames and Data Elements	SAE J2735 Mandatory	CI Implementation
messageId=DE_DSRC_MessageID=19 (SPaT UPER)	M	M
timeStamp=DE_MinuteOfTheYear	O	M
intersections=DF_IntersectionStateList	M	M
id=DF_IntersectionReferenceID	M	M
region=DE_RoadRegulatorID	O	M
id=DE_IntersectionID	M	M
revision=DE_MsgCount	M	M
status=DE_IntersectionStatusObject	M	M
timeStamp=DE_Dsecond	O	M
enabledLanes=DF_EnabledLaneList=1 to 16 x DE_LaneID	O	C (if a revocable lane is active ("enabled") - See Section 4.3.3.3.7)
states=DF_MovementList=1 to 255 x DF_MovementState	M	M
signalGroup=DE_SignalGroupID	M	M
state-time-speed=DF_MovementEventList	M	M
eventState=DE_MovementPhaseState	M	M
timing=DF_TimeChangeDetails	O	M
startTime=DE_TimeMark	O	M
minEndTime=DE_TimeMark	M	M
maxEndTime=DE_TimeMark	O	M
nextTime=DE_TimeMark	O	M

*DE = Data Element, DF = Data Frame

The source for each of the data frames and data elements that comprise the SPaT message broadcasted by the RSU will vary based on how the connected intersection is configured and also what SPaT information message is used between the TSC infrastructure and the RSU. Table 8 contains links to the specific sections in this CI Implementation Guide with the design details for generating that data element value, based on SPaT information message used between the TSC infrastructure and the RSU; whether it is the UPER-encoded SPaT Message or *NTCIP 1202 v03A*. Table 15 shows how a TSCBM may be used to generate a SPaT Message.

Table 8. SPaT Message Data Sources

SAE J2735 Data Element	SAE J2735 SPaT Message	NTCIP 1202 v03A Object Definition
timeStamp (DE_MinuteOfTheYear)	See 4.3.3.2.3	Provided by RSU
id=DF_IntersectionReferenceID	See 4.3.3.3.1	
region=DE_RoadRegulatorID	See 4.3.3.3.1.2	Unsupported

SAE J2735 Data Element	SAE J2735 SPaT Message	NTCIP 1202 v03A Object Definition
id=DE_IntersectionID	See 4.3.3.3.1.3	rsuAscSpatId
revision=DE_MsgCount	See 4.3.3.2.2.1	rsuAscSpatMsgCount
status=DE_IntersectionStatusObject	See 4.3.3.3.2	spatStatus
timeStamp=DE_Dsecond	See 4.3.3.2.3.2	Provided by RSU
enabledLanes=DF_EnabledLaneList	See 4.3.3.3.7	rsuAscSpatEnabledLanes
states=DF_MovementList	See 4.3.3.3.3	
signalGroup=DE_SignalGroupID	See 4.3.3.3.3.1	channelNumber
state-time-speed=DF_MovementEventList		
eventState=DE_MovementPhaseState (Current Movement)	See 4.3.3.3.3	signalState
eventState=DE_MovementPhaseState (Next Movement)	See 4.3.3.3.4	Unsupported
timing=DF_TimeChangeDetails	See 4.3.3.3.5	
startTime=DE_TimeMark	See 4.3.3.3.5.7, 4.3.3.3.5.8	Unsupported
minEndTime=DE_TimeMark	See 4.3.3.3.5.3	signalStateMinEndTick. Provided as ticks to the RSU
maxEndTime=DE_TimeMark	See 4.3.3.3.5.4	signalStateMaxEndTick. Provided as ticks to the RSU
nextTime=DE_TimeMark	See 4.3.3.3.6.1	signalNextTick. Provided as ticks to the RSU

4.3.3.1.1.4 SPaT Message PSID

The PSID for the SPaT message shall be 0x82 (0p80-02). The PSID is used for the destination address in broadcast WSM and in the *app Permissions Field* in the SPaT signing certificate.

See <https://standards.ieee.org/products-programs/regauth/psid/public/>.

4.3.3.1.1.5 MAP Message - SAE J2735

See MSG_MapData (MAP) in *SAE J2735_202007*.

NOTE: This CI Implementation Guide references *SAE J2735_202007*. At the time of publication, most implementations use the *SAE J2735_201603* version. There are some differences between the March 2016 version and the July 2020 version; implementers should be aware of the changes.

4.3.3.1.1.6 MAP Message - Mandatory Data Elements

See MSG_MapData (MAP) in *SAE J2735_202007*.

4.3.3.1.1.7 MAP Message - Required Data Elements

Table 9 lists the data frames (begins with DF_) and the data elements (begins with DE_) in the MSG_MapData (MAP) message of *SAE J2735_202007* are required to be supported to conform to the CI Implementation Guide. The data frames and data elements are nested and listed in the order they appear in the MAP message. All data frames and data elements listed in Table 9 shall be supported by a connected intersection, however, several data frames and data elements do not have to be included in every broadcasted message under certain conditions.

The "SAE J2735 Mandatory" column indicates if the data frame or data element is mandatory to describe the roadway geometry for an intersection as defined in *SAE J2735_202007*. A value of M indicates that the data frame or data element is mandatory, while a value of O indicates that the data frame or data

element is optional. O.# (range) notation indicates that the data frame/element is part of an option group (#), and is used to show a set of selectable options. Support of the number of items indicated by the '(range)' is required from all options labeled with the same numeral #. A value of C indicates the data frame or data element is conditionally mandatory, meaning that the data frame or data element shall be broadcasted if certain conditions are met. The condition is also included in parentheses after the "C."

For example, O.1 (1..*) indicates that one or more of the option group 1 options shall be implemented. Each node point (nodes) must be described by a choice of node-XY1, node-XY2, node-XY3, node-XY4, node-XY5, or node-XY6. The (1..*) indicates that different node points may be described by more than one of the choices (i.e., it doesn't have to be the same choice to describe all the node points).

The "CI Implementation" column indicates which data frames and data elements must be included in the broadcasted MAP message. A value of M indicates the data frame or data element must be included in every MAP message broadcasted. A value of O indicates the data frame or data element does not have to be included in every MAP message broadcasted. A value of C indicates the data frame or data element is conditionally mandatory, meaning that the data frame or data element shall be broadcasted if certain conditions are met.

For example, computed lanes (DF_ComputedLane) may not be needed or applicable to describe a lane associated with an intersection in a MAP message. In those situations, the data frames and data elements describing a computed lane may not be included in the MAP message, even though the connected intersection is capable of providing those data frames and data elements. However, if a computed lane is necessary, then it can be included in the MAP message. If the computed lane data frame (DF_ComputedLane) is included in the MAP message, then the data elements referenceLaneId, offsetXAxis, and offsetYAxis become mandatory and should also be included in the MAP message.

Table 9. MAP Message - Required Elements

SAE J2735 Data Frames and Data Elements	SAE J2735 Mandatory	CI Implementation
messageId=DE_DSRCmsgID=18 (MAP UPER)	M	M
msgIssueRevision=DE_MsgCount	M	M
intersections=DF_IntersectionGeometryList=1 to 32 X DF_IntersectionGeometry	O	M
id=DF_IntersectionReferenceID	M	M
region=DE_RoadRegulatorID	O	M
id=DE_IntersectionID	M	M
revision=DE_MsgCount	M	M
refPoint=DF_Position3D	M	M
lat=DE_Latitude	M	M
long=DE_Longitude	M	M
elevation=DE_Elevation	O	M
laneWidth=DE_LaneWidth	O	M
speedLimits=DF_SpeedLimitList=1 to 9 x DF_RegulatorySpeedLimit	O	M
type=DE_SpeedLimitType	C (if speedLimits is included)	M
speed=DE_Velocity	C (if speedLimits is included)	M
laneSet=DF_LaneList=1 to 255 X DF_GenericLane	M	M
laneID=DE_LaneID	M	M
laneAttributes=DF_LaneAttributes	M	M
directionalUse=DE_LaneDirection	M	M
sharedWith=DE_LaneSharing	M	M

SAE J2735 Data Frames and Data Elements	SAE J2735 Mandatory	CI Implementation
laneType=DF_LaneTypeAttributes (revocable)	M	M
maneuvers=DE_AllowedManeuvers	O	M
nodeList=DF_NodeListXY=Choice of DF_NodeSetXY OR DF_ComputedLane	M	M
nodes= DF_NodeSetXY=2 to 63 X DF_NodeXY	M	M
delta=DF_NodeOffsetPointXY	M	M
node-XY1=DF_Node_XY_20b	O.1 (1..*)	O.4 (1..*)
x=DE_Offset_B10	C (if node-XY1 is included)	C (if node-XY1 is included - See Section 4.3.3.4.1.15)
y=DE_Offset_B10	C (if node-XY1 is included)	C (if node-XY1 is included - See Section 4.3.3.4.1.15)
node-XY2=DF_Node_XY_22b	O.1 (1..*)	O.4 (1..*)
x=DE_Offset_B11	C (if node-XY2 is included)	C (if node-XY2 is included - See Section 4.3.3.4.1.15)
y=DE_Offset_B11	C (if node-XY2 is included)	C (if node-XY2 is included - See Section 4.3.3.4.1.15)
node-XY3=DF_Node_XY_24b	O.1 (1..*)	O.4 (1..*)
x=DE_Offset_B12	C (if node-XY3 is included)	C (if node-XY3 is included - See Section 4.3.3.4.1.15)
y=DE_Offset_B12	C (if node-XY3 is included)	C (if node-XY3 is included - See Section 4.3.3.4.1.15)
node-XY4=DF_Node_XY_26b	O.1 (1..*)	O.4 (1..*)
x=DE_Offset_B13	C (if node-XY4 is included)	C (if node-XY4 is included - See Section 4.3.3.4.1.15)
y=DE_Offset_B13	C (if node-XY4 is included)	C (if node-XY4 is included - See Section 4.3.3.4.1.15)
node-XY5=DF_Node_XY_28b	O.1 (1..*)	O.4 (1..*)
x=DE_Offset_B14	C (if node-XY5 is included)	C (if node-XY5 is included - See Section 4.3.3.4.1.15)
y=DE_Offset_B14	C (if node-XY5 is included)	C (if node-XY5 is included - See Section 4.3.3.4.1.15)
node-XY6=DF_Node_XY_32b	O.1 (1..*)	O.4 (1..*)
x=DE_Offset_B16	C (if node-XY6 is included)	C (if node-XY6 is included - See Section 4.3.3.4.1.15)
y=DE_Offset_B16	C (if node-XY6 is included)	C (if node-XY6 is included - See Section 4.3.3.4.1.15)
attributes=DF_NodeAttributeSetXY	O	O
data=DF_LaneDataAttributeList=1 to 8 x DF_LaneDataAttribute	O	O
DF_LaneDataAttribute=Choice	O	C (if data is included - See Section 4.3.3.4.5.2)
speedLimits=DF_SpeedLimitList=1 to 9 X DF_RegulatorySpeedLimit	O	C (if data is included - See Section 4.3.3.4.5.2)
type=DE_SpeedLimitType	C (if speedLimits is included)	C (if data is included - See Section 4.3.3.4.5.2)
speed=DE_Velocity	C (if speedLimits is included)	C (if data is included - See Section 4.3.3.4.5.2)
dWidth=DE_Offset_B10	O	C (for differences in lane widths - See Section 4.3.3.4.1.22)

SAE J2735 Data Frames and Data Elements	SAE J2735 Mandatory	CI Implementation
dElevation=DE_Offset_B10	O	C (for differences in elevations - See Section 4.3.3.4.1.16)
computed=DF_Computed Lane	O	C (For computed lanes - See Section 4.3.3.1.3.2.2)
referenceLaneId=DE_LaneID	C (if computed is selected)	C (For computed lanes - See Section 4.3.3.1.3.2.2.1)
offsetXaxis=Choice	C (if computed is selected)	C (For computed lanes - See Section 4.3.3.1.3.2.2.2)
small=DE_DrivenLineOffsetSmall	O.2 (1..*) (if computed is selected)	O.7 (1) (For computed lanes - See Section 4.3.3.1.3.2.2.2)
large=DE_DrivenLineOffsetLarge	O.2 (1..*) (if computed is selected)	O.7 (1) (For computed lanes - See Section 4.3.3.1.3.2.2.2)
offsetYaxis=Choice	C (if computed is selected)	C (For computed lanes - See Section 4.3.3.1.3.2.2.3)
small=DE_DrivenLineOffsetSmall	O.3 (1..*) (if computed is selected)	O.8 (1) (For computed lanes - See Section 4.3.3.1.3.2.2.3)
large=DE_DrivenLineOffsetLarge	O.3 (1..*) (if computed is selected)	O.8 (1) (For computed lanes - See Section 4.3.3.1.3.2.2.3)
rotateXY=DE_Angle	O	O (For computed lanes - See Section 4.3.3.1.3.2.2.4)
connectsTo=DF_ConnectsToList=1 to 16 X DF_Connection	O	M
connectingLane=DF_ConnectingLane	C (if connectsTo is selected)	M
lane=DE_LaneID	C (if connectsTo is selected)	M
maneuvers=DE_AllowedManeuver	O	M
signalGroup=DE_SignalGroupID	O	M

Table 10 contains links to the specific sections in this CI Implementation Guide with the design details for generating that data element value.

Table 10. MAP Message Design Details

SAE J2735 Data Frames and Data Elements	CI Implementation
messageId=DE_DSRCmsgID=18 (MAP UPER)	See Section 4.3.3.1.1.5
msgIssueRevision=DE_MsgCount	See Sections 4.3.3.2.2.3 and 4.3.3.2.2.4
intersections=DF_IntersectionGeometryList=1 to 32 X DF_IntersectionGeometry	See Section 4.3.3.4.1.1
id=DF_IntersectionReferenceID	
region=DE_RoadRegulatorID	See Section 4.3.3.4.1.2
id=DE_IntersectionID	See Section 4.3.3.4.1.3
revision=DE_MsgCount	See Sections 4.3.3.2.2.5 and 4.3.3.2.2.6
refPoint=DF_Position3D	See Section 4.3.3.4.1.4
lat=DE_Latitude	See Section 4.3.3.4.1.4
long=DE_Longitude	See Section 4.3.3.4.1.4
elevation=DE_Elevation	See Section 4.3.3.4.1.4
laneWidth=DE_LaneWidth	See Section 4.3.3.4.1.5
speedLimits=DF_SpeedLimitList=1 to 9 x DF_RegulatorySpeedLimit	See Section 4.3.3.4.5.1
type=DE_SpeedLimitType	See Section 4.3.3.4.5.1
speed=DE_Velocity	See Section 4.3.3.4.5.1

SAE J2735 Data Frames and Data Elements	CI Implementation
laneSet=DF_LaneList=1 to 255 X DF_GenericLane	
laneID=DE_LaneID	See Section 4.3.3.4.1.6
laneAttributes=DF_LaneAttributes	
directionalUse=DE_LaneDirection	See Section 4.3.3.4.2.1
sharedWith=DE_LaneSharing	See Section 4.3.3.4.2.2
laneType=DF_LaneTypeAttributes (revocable)	See Section 4.3.3.4.2.3
maneuvers=DE_AllowedManeuvers	See Section 4.3.3.4.3
nodeList=DF_NodeListXY=Choice of DF_NodeSetXY OR DF_ComputedLane	
nodes= DF_NodeSetXY=2 to 63 X DF_NodeXY	See Section 4.3.3.4.1.21
delta=DF_NodeOffsetPointXY	
node-XY1=DF_Node_XY_20b	See Section 4.3.3.4.1.15
x=DE_Offset_B10	See Section 4.3.3.4.1.15
y=DE_Offset_B10	See Section 4.3.3.4.1.15
node-XY2=DF_Node_XY_22b	See Section 4.3.3.4.1.15
x=DE_Offset_B11	See Section 4.3.3.4.1.15
y=DE_Offset_B11	See Section 4.3.3.4.1.15
node-XY3=DF_Node_XY_24b	See Section 4.3.3.4.1.15
x=DE_Offset_B12	See Section 4.3.3.4.1.15
y=DE_Offset_B12	See Section 4.3.3.4.1.15
node-XY4=DF_Node_XY_26b	See Section 4.3.3.4.1.15
x=DE_Offset_B13	See Section 4.3.3.4.1.15
y=DE_Offset_B13	See Section 4.3.3.4.1.15
node-XY5=DF_Node_XY_28b	See Section 4.3.3.4.1.15
x=DE_Offset_B14	See Section 4.3.3.4.1.15
y=DE_Offset_B14	See Section 4.3.3.4.1.15
node-XY6=DF_Node_XY_32b	See Section 4.3.3.4.1.15
x=DE_Offset_B16	See Section 4.3.3.4.1.15
y=DE_Offset_B16	See Section 4.3.3.4.1.15
attributes=DF_NodeAttributeSetXY	
data=DF_LaneDataAttributeList=1 to 8 x DF_LaneDataAttribute	
DF_LaneDataAttribute=Choice	
speedLimits=DF_SpeedLimitList=1 to 9 X DF_RegulatorySpeedLimit	See Section 4.3.3.4.5.2
type=DE_SpeedLimitType	See Section 4.3.3.4.5.2
speed=DE_Velocity	See Section 4.3.3.4.5.2
dWidth=DE_Offset_B10	See Section 4.3.3.4.1.22
dElevation=DE_Offset_B10	See Section 4.3.3.4.1.16
computed=DF_Computed Lane	See Section 4.3.3.1.3.2.2
referenceLaneID=DE_LaneID	See Section 4.3.3.1.3.2.2.1
offsetXaxis=Choice	See Section 4.3.3.1.3.2.2.2
small=DE_DrivenLineOffsetSmall	See Section 4.3.3.1.3.2.2.2
large=DE_DrivenLineOffsetLarge	See Section 4.3.3.1.3.2.2.2
offsetYaxis=Choice	See Section 4.3.3.1.3.2.2.3
small=DE_DrivenLineOffsetSmall	See Section 4.3.3.1.3.2.2.3
large=DE_DrivenLineOffsetLarge	See Section 4.3.3.1.3.2.2.3
rotateXY=DE_Angle	See Section 4.3.3.1.3.2.2.4
connectsTo=DF_ConnectsToList=1 to 16 X DF_Connection	See Section 4.3.3.4.4.1
connectingLane=DF_ConnectingLane	See Section 4.3.3.4.4.1
lane=DE_LaneID	See Section 4.3.3.4.4.2
maneuvers=DE_AllowedManeuver	See Section 4.3.3.4.4.3
signalGroup=DE_SignalGroupID	See Section 4.3.3.4.4.4

4.3.3.1.1.8 MAP Message PSID

The PSID for the MAP message shall be 0x20-40-97 (0pE0-00-00-17). The PSID is used for the destination address in broadcast WSM and in the *app Permissions Field* in the MAP signing certificate.

See <https://standards.ieee.org/products-programs/regauth/psid/public/>.

4.3.3.1.1.9 RTCMcorrections Message - SAE J2735

See MSG_RTCMcorrections (RTCM) in *SAE J2735_202007*.

4.3.3.1.1.10 RTCMcorrections Message - Mandatory Data Elements

See MSG_RTCMcorrections (RTCM) in *SAE J2735_202007*.

4.3.3.1.1.11 RTCMcorrections Message - Required Data Elements

Table 11 lists the data frames (begins with DF_) and the data elements (begins with DE_) in the MSG_RTCMcorrections (RTCM) of *SAE J2735_202007* are mandatory to be supported to conform to the CI Implementation Guide. The data frames and data elements are listed in the order it appears in the RTCMcorrections message.

The "SAE J2735 Mandatory" column indicates if the data frame or data element is mandatory as defined in *SAE J2735_202007*. A value of M indicates that the data frame or data element is mandatory, while a value of O indicates that the data frame or data element is optional.

The "CI Implementation" column indicates which data frames and data elements shall be included in the broadcasted RTCMcorrections message. A value of M indicates the data frame or data element shall be included in every RTCMcorrections message broadcasted. All other data frames and data elements available in SAE J2735 shall not be included in RTCMcorrections.

Table 11. RTCMcorrections Message - Required Elements

SAE J2735 Data Frames and Data Elements	SAE J2735 Mandatory	CI Implementation
messageId=DE_DSRCmsgID=28 (RTCM UPER)	M	M
msgCnt = DE_MsgCount	M	M
rev=RTCM-Revision	M	M
anchorPoint=DF_FullPositionVector	O	M
msgs=DF_RTCMmessageList	M	M

Design details for the data frames and data elements for the RTCMcorrections Message can be found in Section 4.3.3.5.1.

4.3.3.1.1.12 RTCMcorrections Message PSID

The PSID for the RTCMcorrections message shall be 0x80 (0p80-00). The PSID is used for the destination address in broadcast WSM and in the *app Permissions Field* in the RTCMcorrections signing certificate.

See <https://standards.ieee.org/products-programs/regauth/psid/public/>.

4.3.3.1.2 Robustness Design Details

The design details to fulfill the requirements for a connected intersection to operate under different degraded conditions follow. These requirements are defined in Section 3.3.3.1.2.

4.3.3.1.2.1 Broadcast SPaT Message Design Details

Multiple elements in the SPaT message are mandatory to be broadcasted according to *SAE J2735_202007* and to conform to this CI Implementation Guide. Table 7 indicates which data frames and elements are mandatory.

A SPaT message shall be broadcasted for an intersection if ALL the following conditions are met:

- The SPaT message contains a valid Intersection reference identifier (DE_RoadRegulatorID + DE_IntersectionID)
- The SPaT message contains a valid revision object (DE_MsgCount)
- The SPaT message contains a valid intersection status object (DE_IntersectionStatusObject)
- The SPaT message contains a valid timeStamp (DE_Dsecond and DE_MinuteOfTheYear)
- The SPaT message is protected based on the *IEEE Std 1609.2-2016* security profile for SPaT messages (See Section 3.3.4.6.3, Interface between an RSU and the OBU/MU)
- The requirements for Sections 3.3.3.4.8.1, Matching Intersection Reference Identifier and 3.3.3.4.8.2, Matching SPaT and MAP Version are fulfilled.

All other data elements required to be included in the SPaT message by the CI Implementation Guide may use a value of unavailable, unknown, or not known as appropriate.

4.3.3.1.3 Concise Messages Design Details

The design details to fulfill the requirements to provide complete data describing the situation within the maximum message size supported by the communications stack follow. The requirements are defined in Section 3.3.3.1.3.

4.3.3.1.3.1 Transport Message Size - WAVE

The default maximum transport message in *IEEE Std 1609.3-2020* for a WAVE Short Message (WSM) payload is 1400 bytes; however a maximum of 2302 bytes is supported. SPaT and MAP messages sent over a DSRC V2X interface must be less than 2302, including security overhead (signature, certificate and header). Note that the maximum value of the WSM payload may need to be configured / set to 2302 to support larger MAP messages if the implementer is using the *IEEE Std 1609.3 MIB*.

For C-V2X, 8000 bytes is the maximum payload including security overhead, but implementers are encouraged to keep SPaT and MAP messages as small as possible for both CV2X and DSRC to maximize reliability of reception.

4.3.3.1.3.2 Concise MAP Message Design Details

The design details to fulfill the requirements for concise MAP messages follow. The requirements are defined in Section 3.3.3.1.3.2.

4.3.3.1.3.2.1 Nodes by Offsets

Although *SAE J2735_202007* allows describing the location of a node point of a lane using absolute latitude or longitude values, using offsets results in a more compact MAP message size. Using only offsets from an intersection reference point or a previous node point also simplifies the processing an OBU/MU must perform to understand the MAP message.

4.3.3.1.3.2.2 Computed Lane Design Details

The design details for requirements for a computed lane follow. The requirements are defined in Section 3.3.3.1.3.2.2.

4.3.3.1.3.2.2.1 Computed Lane - Lane Identifier

The lane identifier of the reference lane for a computed lane is represented as `referenceLaneId` (`DE_LaneId`) and can be found under the data frame `DF_ComputedLane` in the `MSG_MapData` message in *SAE J2735_202007*. All node attributes defined for the reference lane are also inherited by the computed lane.

Generally, computed lanes are used at intersections where adjacent lanes of the same width are entering or exiting the intersection. The left-most lane in the direction of traffic is recommended as the reference lane. The right-most lane (in the direction of traffic) generally has to consider permitted parking.

Be aware of potential issues with defining an adjacent lane as a computed lane when the referenced lane includes a change in the lane width. It is not clear how the lanes would contract or expand in width with adjacent lanes. Also, no guidance is provided at this time when the referenced lane includes sharp curves.

4.3.3.1.3.2.2.2 Computed Lane - X-Offset

The X-offset describes the difference, in centimeters, along the east-west axis between the first node point of the referenced lane to the first node point of the computed lane. Positive X offsets are to the east. The x-offset for a computed lane from a referenced lane is represented as `offsetXaxis` and can be found under the data frame `DF_ComputedLane` in the `MSG_MapData` message in *SAE J2735_202007*. `offsetXaxis` is a choice between `DE_DrivenLineOffsetSmall` or `DE_DrivenLineOffsetLarge`, the difference between the data elements is the size of the data elements. `DE_DrivenLineOffsetSmall` requires 12 bits of data and supports offsets up to 2047 centimeters to the east or west. `DE_DrivenLineOffsetLarge` requires 16 bits of data and supports offsets up to 32,767 centimeters.

If the x-offset between the computed lane and the reference lane is less than 2047 centimeters, `DE_DrivenLineOffsetSmall` should be used.

Figure 16 illustrates an example of computed lanes for intersection mapping. In Figure 16, lanes #5, #15, #17 and #21 are computed from a reference (source) lane #3. The first node point for the computed lane is represented as X and Y offsets in centimeters as a green square from the first node point of the reference lane #3. In this example, the lane width is assumed as 360 centimeters and the width of the intersection as 1500 centimeters.

The node attributes associated with the reference lane cannot be changed for the computed (target) lanes.

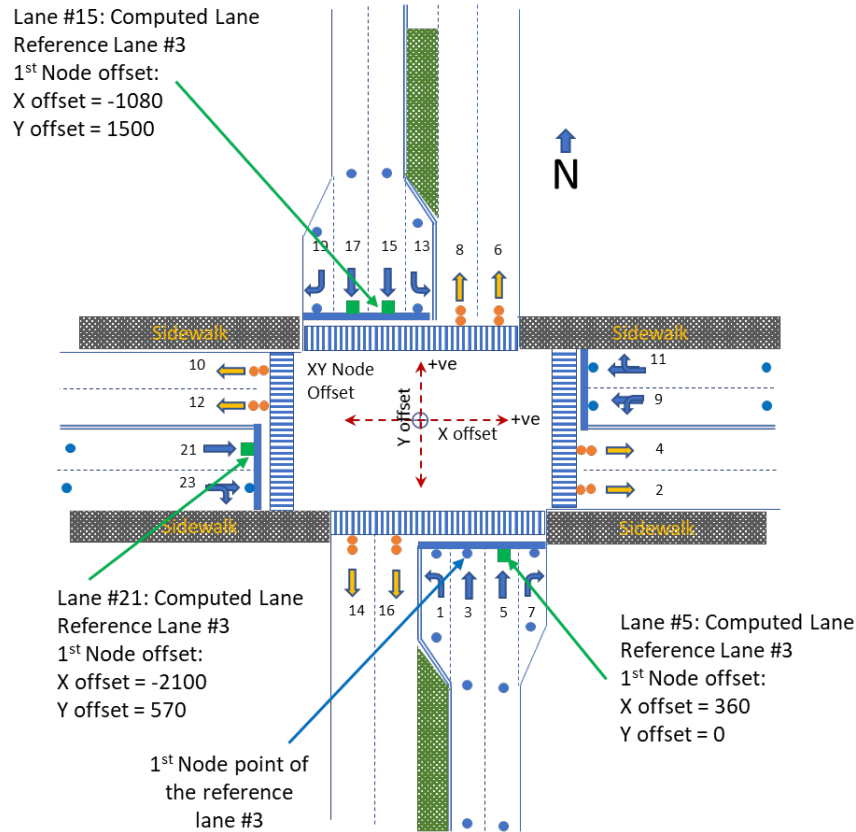


Figure 16. Computed Lane.

The computed lane representation for lanes 5, 15 and 17 (The lane attributes are not shown) using JSON encoding are the following:

```
{"laneID":5,"laneAttributes":{...},"maneuvers":"8000","nodeList":{"computed":[{"referenceLaneID":3,"offsetXaxis":360,"offsetYaxis":0}]}}
```

```
{"laneID":15,"laneAttributes":{...},"maneuvers":"8000","nodeList":{"computed":[{"referenceLaneID":3,"offsetXaxis":-1080,"offsetYaxis":1500,"rotateXY":14400}]}}
```

```
{"laneID":21,"laneAttributes":{...},"maneuvers":"8000","nodeList":{"computed":[{"referenceLaneID":3,"offsetXaxis":-2100,"offsetYaxis":570,"rotateXY":7200}]}}
```

4.3.3.1.3.2.2.3 Computed Lane - Y-Offset

The y-offset describes the difference, in centimeters, along the north-south axis between the first node point of the referenced lane to the first node point of the computed lane. Positive Y offsets are to the north. The y-offset for a computed lane from a referenced lane is represented as offsetYaxis and can be found under the data frame DF_ComputedLane in the MSG_MapData message in SAE J2735_202007. offsetYaxis is a choice between DE_DrivenLineOffsetSmall or DE_DrivenLineOffsetLarge, the difference between the data elements is the size of the data elements. DE_DrivenLineOffsetSmall requires 12 bits of data and supports offsets up to 2047 centimeters to the east or west. DE_DrivenLineOffsetLarge requires 16 bits of data and supports offsets up to 32,767 centimeters.

If the y-offset between the computed lane and the reference lane is less than 2047 centimeters, DE_DrivenLineOffsetSmall should be used.

See Figure 16 for an example illustration of a computed lane, including a sequence using JSON encoding.

4.3.3.1.3.2.2.4 Computed Lane - Angle

If the computed lane is oriented at a different angle from the referenced lane, the angle of the rotation value is represented as rotateXY (DE_Angle) and can be found under the data frame DF_ComputedLane in the MSG_MapData message in *SAE J2735_202007*. The rotation value is expressed as unsigned units of 0.0125 degrees (from 0 to 359.9875 degrees), with positive values to the "East" if the orientation of the lane is to the North (or to the right in the direction the traveler is facing).

The JSON encoding sequence for lane numbers 15 and 17 that follow Figure 16 are examples of how angle is presented in a computed lane.

4.3.3.1.4 Advanced Notification Design Details

The design details to fulfill the requirements to provide data far enough in advance of the intersection so the application on an OBU/MU can process the data in time to react to a situation follow. The requirements are defined in Section 3.3.3.1.4.

4.3.3.1.4.1 Data Coverage - Every Lane

This requirement requires that an OBU/MU in any lane approaching the intersection can receive the messages broadcasted by the connected intersection. Also see the next design detail section, 4.3.3.1.4.2.

4.3.3.1.4.2 Advanced Notification - Time

This requirement is verified (tested) by demonstration.

4.3.3.1.5 Timeliness Design Details

The design details to fulfill the requirements for indicating changes in state, timing, and physical indications follow. The requirements are defined in Section 3.3.3.1.5.

4.3.3.1.5.1 SPaT Message - Broadcast Periodicity

No design details provided at this time.

4.3.3.1.5.2 SPaT Message - Broadcast Latency

The latency is defined as from the time when the signals are commanded to change is asserted by the traffic signal controller to change the signal head indication, to when the SPaT message with the change in signal indication (movement state) is received by the OBU/MU.

The verification is performed by test.

For verification testing, the epoch of the OBU when the message is received will be compared to the timestamp in the SPaT message, but this test only verifies the latency between the RSU and OBU.

4.3.3.1.5.3 MAP Message - Broadcast Periodicity

No design details provided at this time.

4.3.3.1.6 Quality Assurance Design Details

The design details to fulfill the requirements to provide quality information follow. These requirements are defined in Section 3.3.3.1.6.

4.3.3.1.6.1 Completeness - SPaT Message

This requirement is fulfilled all movements controlled by the TSC infrastructure and included in the associated MAP message is represented in the SPaT message. This is defined as when every allowed movement in every ingress lane into the intersection is controlled and may have one or more movement state, as represented by DE_MovementPhaseState. This includes pedestrian movements, bicycle movements, and tracked vehicle movements that are controlled by the TSC infrastructure.

This requirement is verified by inspection.

4.3.3.1.6.2 Completeness - MAP Message

For a connected intersection, this requirement is fulfilled when the ingress lane and egress lane for every allowed movement through the intersection and controlled by the TSC infrastructure is represented in the MAP message. This includes all pedestrian crosswalks, bicycle lanes, and tracked vehicle lanes whose movements are controlled by the TSC infrastructure.

This requirement is verified by inspection.

4.3.3.2 Generic Message Design Details

The design details to fulfill requirements for a connected intersection transmitting data follow. These requirements are defined in Section 3.3.3.2.

4.3.3.2.1 Time Accuracy

This requirement is verified by testing.

4.3.3.2.2 Message Revision Counter Design Details

The design details to fulfill the requirements to see if the data transmitted by a connected intersection is new follow. These requirements are defined in Section 3.3.3.2.2.

4.3.3.2.2.1 SPaT Message - Revision Counter Increment

The revision counter for a SPaT message is represented by revision (DE_MsgCount) and found under the data frame DF_IntersectionState in MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*.

The revision counter shall remain the same during a stream of messages when the content within each message has not changed except the timestamp from the prior message sent. The OBU/MU may ignore processing a new message in the stream if the revision count has not changed from the prior message.

This requirement is verified by inspection.

4.3.3.2.2.2 SPaT Message - Revision Counter Not Increment

This requirement is tested by inspection.

4.3.3.2.2.3 MAP Message - Revision Counter Increment

The revision counter for a MAP message is represented by msgIssueRevision (DE_MsgCount) and found in the MSG_MapData message in *SAE J2735_202007*.

This requirement is verified by inspection.

4.3.3.2.2.4 MAP Message - Revision Counter Not Increment

This requirement is verified by inspection.

4.3.3.2.2.5 MAP Message - Intersection Revision Counter Increment

The revision counter for the geometric description of an intersection is represented by revision (DE_MsgCount) and found under the data frame DF_IntersectionGeometry in the MSG_MapData message in *SAE J2735_202007*.

This requirement is verified by inspection.

4.3.3.2.2.6 MAP Message - Intersection Revision Counter Not Increment

This requirement is verified by inspection.

4.3.3.2.2.7 RTCMcorrections Message - Sequence Number Increment

The sequence number of a RTCMcorrections message is provided by msgCnt (DE_MsgCount) and found in the MSG_RTCMcorrections message in *SAE J2735_202007*. MsgCount shall be incremented when the contents of RTCMmessageList changes.

This requirement is verified by inspection.

Note: RTCMmessageList is a sequence of RTCMmessage containers. If **any** information within **any** those containers changes, MsgCount is incremented. RTCM corrections information changes rapidly, and as a result, so does MsgCount.

4.3.3.2.2.8 RTCMcorrections Message - Sequence Number Not Increment

This requirement is verified by inspection.

4.3.3.2.3 Timestamp Design Details

The design details to fulfill the requirements for a timestamp in messages transmitted by a connected intersection follow. These requirements are defined in Section 3.3.3.2.3.

4.3.3.2.3.1 SPaT Message - Message Time Stamp

The timestamp indicating the minute of the year when the SPaT message was created is represented by timestamp (DE_MinuteOfTheYear) and found in the MSG_SignalPhaseAndTiming Message fulfill in *SAE J2735_202007*.

4.3.3.2.3.2 SPaT Message - Intersection Time Stamp

The timestamp indicating the milliseconds within the current minute when the SPaT message was created is represented by timestamp (DE_DSecond) and found under the data frame DF_IntersectionState in the MSG_SignalPhaseAndTiming Message Dedekind in *SAE J2735_202007*.

4.3.3.3 Signal Timing Data Design Details

The design details to fulfill the requirements for signal timing data broadcasted by a connected intersection follow. The requirements are defined in Section 3.3.3.3.

4.3.3.3.1 Intersection Identification Design Details

The design to provide a unique identifier for an intersection follow. These requirements are defined in Section 3.3.3.3.1.

4.3.3.3.1.1 Intersection Signal Timing Information

Signal phase and timing information for an intersection is represented by intersections (DF_IntersectionStateList) in the MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*.

4.3.3.3.1.2 Road Regulator Identifier

The road regulator identifier is represented as region (DE_RoadRegulatorID) and found under the data frame DF_IntersectionReferenceID in MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*.

The following is a recommendation until a standards development organization agrees to create and maintain a registry for road regulator identifiers. The CI Committee considered various proposals to assign road regulator identifiers, including a proposal by ISO TC 204, but none of the viable proposals were able to fit within the value range currently allowed by *SAE J2735_202007* for road regulator identifiers. A comment has been forwarded to the SAE Core Technical Committee responsible for *SAE J2735_202007* to provide a road regulator identifier field with a sufficient range to support existing jurisdiction codes (See Annex H.1.5).

From *SAE J2735_202007*, road regulator identifiers are values from 0 to 65535, with the value of 0 reserved for testing. These values need to support road regulator identifiers for all of the contiguous North America. The recommendation is as follows:

- 0 = Value for testing
- 1 – 99 = Reserved for future special values
- 100 – 19,999 = To be assigned by Canada at its discretion
- 20,000 – 36,800 = Assigned as per formula below for US states and District of Columbia
- 36,801 – 39,999 = Reserved for future designation in the US
- 40,000 – 59,999 = To be assigned by Mexico and Central American countries at their discretion
- 60,000 – 65,534 = Reserved for future designation
- 65,535 = Reserved for future special value

For the United States, each state and District of Columbia gets one statewide road regulator ID and 299 additional road regulator IDs to designate at their discretion (Note that Texas has 254 counties).

Each state department of transportation is assigned a road regulator ID = 19,700 + (300 * STATE_NUMERIC code from Geographic Names Information System (GNIS) [formerly called the Federal Information Processing Standard (FIPS) code]).

Each state is also assigned an additional 299 sequential road regulator ID codes following the state department of transportation road regulator ID. An agency should reach out to their state DOT to be assigned a road regulator ID at this time.

Note that STATE_NUMERIC (FIPS) codes 03, 07, 14, 43, and 52 are not assigned to states or the District of Columbia. The 300 road regulator IDs that would correspond to each of those codes are reserved for future designation in the United States.

NOTE: At the time of publication, SAE is revisiting the DE_RoadRegulatorID concept using an object identifier (OID) based data structure based on GNIS but the solution has not been approved yet.

4.3.3.3.1.3 Intersection Reference Identifier

The intersection reference identifier is represented as id (DE_IntersectionID) and found under the data frame DF_IntersectionReferenceID in MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*.

The intersection reference identifier is assigned by the IOO represented by the road regulator identifier and is unique within the road regulator identifier.

4.3.3.3.2 Intersection Status Design Details

The design details to fulfill the requirements to provide the status of a connected intersection follow. These requirements are defined in Section 3.3.3.3.2.

4.3.3.3.2.1 Manual Control

Whether the intersection is operating under manual control is represented by Bit 0 in the DE_IntersectionStatusObject and found under the data frame DF_IntersectionState in MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*.

A value of 1 for Bit 0 indicates that the intersection is operating under manual control. Those conditions are defined in Section 4.3.2.2.1.

4.3.3.3.2.2 Stop Time

Whether a signalized intersection has stopped timing for traffic operations is represented by Bit 1 in the DE_IntersectionStatusObject and found under the data frame DF_IntersectionState in MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*.

A value of 1 for Bit 1 indicates that timing has stopped for the signalized intersection. The conditions for stop time are defined in Section 4.3.2.2.2.

4.3.3.3.2.3 Failure Flash

Whether a signalized intersection is in exception (failure) flash is represented by Bit 2 in the DE_IntersectionStatusObject and found under the data frame DF_IntersectionState in MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*.

A value of 1 for Bit 2 indicates that the signalized intersection is in exception flash. The conditions for exception flash are defined in Section 4.3.2.2.3.

While the TSC infrastructure may be aware of several forms of failure flash, it may not be aware of all forms of failure flash, depending on how the connected intersection is wired. For example, the TSC infrastructure may not be aware of a cabinet flash or a conflict flash. Separate wiring may be needed so that the RSU or the TSC infrastructure is aware of a cabinet/conflict/failure flash, depending on where the UPER-encoded SPaT message is generated. This may be addressed in a future version of the CI Implementation Guide.

Note: This may not be possible in an unmodified TS-1 cabinet. It may be possible for this to work for a TS2 controller in a TS1 cabinet.

4.3.3.3.2.4 Preemption

Whether a signalized intersection is in preemption mode is represented by Bit 3 in the DE_IntersectionStatusObject and found under the data frame DF_IntersectionState in MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*.

A value of 1 for Bit 3 indicates that the traffic signal controller is in preemption mode. The definition for preemption mode is in Section 4.3.2.2.5.

4.3.3.3.2.5 Priority

Whether a signalized intersection is servicing a priority request is represented by Bit 4 in the DE_IntersectionStatusObject and found under the data frame DF_IntersectionState in MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*.

A value of 1 for Bit 4 indicates that the traffic signal controller is servicing a priority request, as defined in Section 4.3.2.2.6.

4.3.3.3.2.6 Fixed Time

Whether a signalized intersection is operating in fixed time mode is represented by Bit 5 in the DE_IntersectionStatusObject and found under the data frame DF_IntersectionState in MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*.

A value of 1 for Bit 5 indicates that the traffic signal controller is operating in fixed time, as defined in Section 4.3.2.2.7.

4.3.3.3.2.7 Traffic Dependent Mode

Whether a signalized intersection that is operating in a traffic dependent mode is represented by Bit 6 in the DE_IntersectionStatusObject and found under the data frame DF_IntersectionState in MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*.

A value of 1 for Bit 6 indicates that the traffic signal controller is operating in a non-fixed time mode, as defined in Section 4.3.2.2.8.

Note that the traffic signal controller cannot operate in Traffic Dependent Mode and Fixed Time (Section 4.3.3.3.2.6) at the same time.

4.3.3.3.2.8 Standby Mode

Whether a signalized intersection that is operating in operational flash (standby mode) is represented by Bit 7 in the DE_IntersectionStatusObject and found under the data frame DF_IntersectionState in MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*.

A value of 1 for Bit 7 indicates that the traffic signal controller is in operational flash, as defined in Section 4.3.2.2.4.

4.3.3.3.2.9 Failure Mode

Whether a signalized intersection is in a failure mode is represented by Bit 8 in the DE_IntersectionStatusObject and found under the data frame DF_IntersectionState in MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*.

A value of 1 for Bit 8 indicates that the TSC infrastructure is in failure mode.

A signalized intersection may be considered in a failure mode when the intersection is in a hard flash condition. See Annex A.2.1.6, Hard Flashing Operation and A.2.1.7, Tech Flash.

4.3.3.3.2.10 Controller Off

Whether an RSU is receiving valid data from the TSC infrastructure is represented by Bit 9 in the DE_IntersectionStatusObject and found under the data frame DF_IntersectionState in MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*.

A value of 1 for Bit 9 indicates that the RSU is not receiving valid SPaT information messages from the TSC infrastructure within the last 0.3 seconds.

Note: if the TSC infrastructure generates the UPER-encoded *SAE J2735_202007* SPaT message, and the controller is off, no SPaT message will be generated.

4.3.3.3.2.11 Recent MAP Update

Whether an RSU is broadcasting a new MAP message is represented by Bit 10 in the DE_IntersectionStatusObject and found under the data frame DF_IntersectionState in MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*.

A value of 1 for Bit 10 indicates that the MAP message transmitted by the RSU has recently been updated. However, in practice this bit is not expected to be used by RLVW applications on OBUs. RLVW applications are expected to use the revision counter in the MAP message to determine if there are changes in the MAP messages.

Bit 10 shall be set to a value of 1.

Note: the MAP message can be broadcasted without a SPaT message, but the SPaT message must be sent with a MAP message describing the intersection associated with the SPaT message.

4.3.3.3.2.12 New Lane IDs

Whether an RSU is broadcasting a MAP message with changes in lane assignments or which lanes are enabled in the SPaT message is represented by Bit 11 in the DE_IntersectionStatusObject and found under the data frame DF_IntersectionState in MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*.

A value of 1 for Bit 11 indicates that the lane definitions in the MAP message or the enabled lanes in the SPaT message transmitted by the RSU has recently been updated. However, in practice this bit is not expected to be used by RLVW applications on OBUs. RLVW applications are expected to use the revision counter in the SPaT and MAP message to determine if there are changes in either message.

Bit 11 shall be set to a value of 1.

4.3.3.3.2.13 No MAP Available

Whether an RSU is broadcasting a valid MAP message is represented by Bit 12 in the DE_IntersectionStatusObject and found under the data frame DF_IntersectionState in MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*.

A value of 0 for Bit 12 indicates that the RSU is broadcasting a properly formatted MAP message with a PSID of 0px20-40-97, and a valid *IEEE Std 1609.2-2016* certificate. A value of 1 for Bit 12 indicates that either the MAP is unavailable, or it is invalid. Situations when a MAP may be invalid include temporary lane closures, when the RSU may still be transmitting the MAP message since the IOO may not have

been notified by the contractor for lane closure or time lags. This applies when contractor is setting up cones/barrels for lane closures, presence of flaggers, etc.

A MAP message can be broadcasted without a SPaT message, but the SPaT message must be sent with a valid MAP message describing the intersection associated with the SPaT message. However, there are scenarios when the intersection is operating properly, but the IOO decides not to generate MAP message, maybe for operational or maintenance purposes or the MAP message doesn't have a valid *IEEE Std 1609.2-2016* certificate.

Note: If the UPER-encoded SAE J2735_202007 SPaT message is generated by the TSC infrastructure and the MAP message is generated elsewhere, the TSC infrastructure must be informed if the RSU is broadcasting a MAP message to properly set Bit 12. Note the CI Implementation Guide does not define a requirement for the TSC infrastructure to be informed if a new MAP message is being broadcasted.

4.3.3.3.2.14 No SPaT Available

Whether an RSU is broadcasting a valid SPaT message is represented by Bit 13 in the DE_IntersectionStatusObject and found under the data frame DF_IntersectionState in MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*.

An RSU (or the TSC infrastructure) may set Bit 13 to 1 if the signalized intersection is under test and is not broadcasting a valid SPaT message. An RSU may also set Bit 13 to 1 if the RSU is not receiving valid SPaT information messages from the TSC infrastructure within the last 300 milliseconds.

Note: If the TSC infrastructure generates the UPER-encoded SAE J2735_202007 SPaT message and if the controller is off, no SPaT message will be generated.

4.3.3.3.3 Current Movement State Design Details

The design details to fulfill the requirements for the current movement state of a signal group follow. These requirements are defined in Section 3.3.3.3.3.

4.3.3.3.3.1 Current Movement State for a Signal Group

The state of a movement through an intersection is represented as eventState (DE_MovementPhaseState) and found under data frame DF_MovementEvent in MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*.

Each movement is tied to an identifier called the signalGroup (DE_SignalGroupID), which represents a collection of movements of a common type through the intersection.

If the signal group does not correspond to an actual signal head and therefore is not in the MAP message, then sending information about that fictitious signal group is prohibited.

If the signal group does correspond to an actual signal head and is in the MAP message, then the current movement state has to be sent, even if the current movement state is dark (1). An application will be expecting a state for signal group since it is in the MAP message.

4.3.3.3.3.2 Unknown Current Movement State for a Signal Group

If the current state of a movement through an intersection is unknown, it is represented by a value of unavailable (0) for the eventState (DE_MovementPhaseState), found under data frame DF_MovementEvent in MSG_SignalPhaseAndTiming Message as defined in *SAE J2735_202007*.

4.3.3.3.3 Flashing Yellow Arrow Permissive Movement

A flashing yellow arrow for a permissive movement is represented by a value of permissive-Movement-Allowed (5) for the eventState (DE_MovementPhaseState), found under data frame DF_MovementEvent in MSG_SignalPhaseAndTiming Message as defined in *SAE J2735_202007*.

4.3.3.3.4 Protected and Permissive Clearance

A clearance state immediately following a protected-Movement-Allowed is represented by a value of protected-clearance (8) for the eventState (DE_MovementPhaseState), found under data frame DF_MovementEvent in MSG_SignalPhaseAndTiming Message as defined in *SAE J2735_202007*.

A clearance state immediately following a permissive-Movement-Allowed is represented by a value of permissive-clearance (7) for the eventState (DE_MovementPhaseState), found under data frame DF_MovementEvent in MSG_SignalPhaseAndTiming Message as defined in *SAE J2735_202007*.

4.3.3.3.5 Resolve Protected Versus Permissive Movement

An allowed movement that is in conflict with another movement is represented by a value of permissive-Movement-Allowed (5) for the eventState (DE_MovementPhaseState), as defined in *SAE J2735_202007*; and represented by a value of protected-Movement-Allowed (6) when the same allowed movement is not in conflict with another movement.

Note that there is some question if *NTCIP 1202 v03A* currently addresses protected and permissive movements correctly as stated. The question has been posed to the NTCIP Actuated Signal Controllers Working Group. See Annex H.2.1, Protected / Permissive Movements. In the mean time, the RSU could be configured to resolve the protected permissive state of a protected permissive signal group in the same way that it does not for TSCBM. The controller could send the state of the protected movement channel and the permissive movement channel/overlap and the RSU could resolve it using a custom configured table.

Also, while the TSCBM can indicate if the current movement state is green, yellow or red, it does not indicate if the movement allowed or the clearance state is a protected movement/clearance or a permissive movement/clearance. The RSU receiving the TSCBM has to be configured to determine when a phase or overlap movement is protected or permissive. There is currently no standardized interface to configure this information.

4.3.3.3.6 Conflict Causes Permissive

An allowed movement that is in potential conflict with another movement is represented by a value of permissive-Movement-Allowed (5) for the eventState (DE_MovementPhaseState), found under data frame DF_MovementEvent in MSG_SignalPhaseAndTiming Message as defined in *SAE J2735_202007*.

4.3.3.3.7 No Conflict Causes Protected

An allowed movement that does not conflict with another movement is represented by a value of protected-Movement-Allowed (6) for the eventState (DE_MovementPhaseState), found under data frame DF_MovementEvent in MSG_SignalPhaseAndTiming Message as defined in *SAE J2735_202007*.

4.3.3.3.8 WALK State Enumeration (No Conflict)

A pedestrian WALK interval that has no conflict with a vehicle movement is represented by a value of protected-Movement-Allowed (6) for the eventState (DE_MovementPhaseState), found under data frame DF_MovementEvent in MSG_SignalPhaseAndTiming Message as defined in *SAE J2735_202007*.

NOTE: A WALK may have no conflict for part of its duration and change to having a conflict. For example, a leading pedestrian interval brings up the WALK indication for a few seconds before the parallel vehicle movements gets a permissive green that includes turning movements in conflict with the WALK.

4.3.3.3.9 WALK State Enumeration (Potential Conflict)

A pedestrian WALK interval that is in conflict with a vehicle movement is represented by a value of permissive-Movement-Allowed (5) for the eventState (DE_MovementPhaseState), found under data frame DF_MovementEvent in MSG_SignalPhaseAndTiming Message as defined in *SAE J2735_202007*.

4.3.3.3.10 Flashing DON'T WALK State Enumeration

A pedestrian Flashing DON'T WALK interval that may be in conflict with another movement is represented by a value of permissive-clearance (7) for the eventState (DE_MovementPhaseState), found under data frame DF_MovementEvent in MSG_SignalPhaseAndTiming Message as defined in *SAE J2735_202007*.

A pedestrian Flashing DON'T WALK interval that has no conflict with another movement is represented by a value of protected-clearance (8) for the eventState (DE_MovementPhaseState), found under data frame DF_MovementEvent in MSG_SignalPhaseAndTiming Message as defined in *SAE J2735_202007*.

4.3.3.3.11 Steady DON'T WALK State Enumeration

A pedestrian Steady DON'T WALK interval is represented by a value of stop-And-Remain (3) for the eventState (DE_MovementPhaseState), found under data frame DF_MovementEvent in MSG_SignalPhaseAndTiming Message as defined in *SAE J2735_202007*.

4.3.3.3.4 Next Movement State Design Details

The design details to fulfill the requirements for the next movement state of a signal group follow. These requirements are defined in Section 3.3.3.3.4.

4.3.3.3.4.1 Next Movement State

MSG_SignalPhaseAndTiming Message provides a data frame, DF_MovementEventList, that contains 1 to 16 entries for the same movement at an intersection. Each entry (represented by DF_MovementEvent) represents a movement state for that movement over a period of time.

- The first entry describes the current movement state (i.e., DE_MovementPhaseState) and the time change details for the current movement (minEndTime, maxEndTime, and nextTime).
- The second entry describes the movement state immediately after the current movement state terminates; and the start, minimum end, and maximum end times (i.e., startTime, minEndTime, and maxEndTime) for the next movement state.

If the TSC infrastructure knows the next movement state, the TSC infrastructure shall provide the next movement state in the second entry of DF_MovementEventList, as eventState (DE_MovementPhaseState), found under data frame DF_MovementEvent in MSG_SignalPhaseAndTiming Message as defined in *SAE J2735_202007*.

If the next movement state, as represented by DE_MovementPhaseState, is unknown, a second entry for the movement (DF_MovementEvent) shall be sent in DF_MovementEventList as unknown. Note that during an AGP, the next movement state is known and is broadcasted.

For example, in Figure 17, lane #1 is tied to signal group #2 and currently a permitted left turn (FY (Flashing Yellow) in Figure 17). The minimum end time for signal group 2 is currently 34675 deciseconds and the maximum end time is 35244 deciseconds from the top of the hour. At this point in time, the TSC

infrastructure has not determined if the next movement state is a clearance interval or a protected left turn. So, the SPaT message for this movement would be the following:

```
{ "signalGroup":2, "state-time-speed":[{ "eventState":"permissive-Movement-Allowed", "timing":{"minEndTime":34675, "maxEndTime":35244}}, { "eventState":"unavailable", "timing":{"startTime":36111, "minEndTime":36111, "maxEndTime":36111}}]}
```

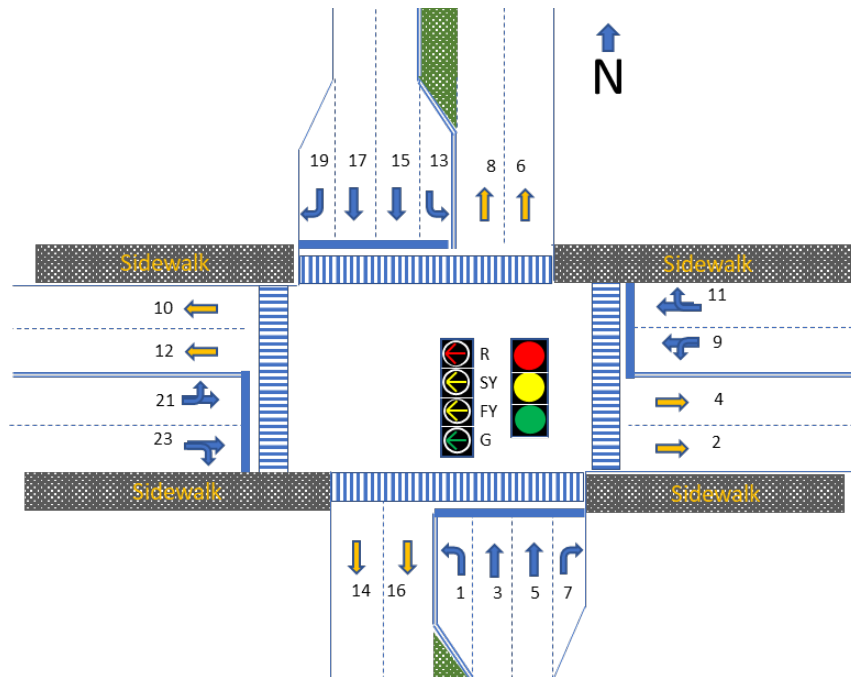


Figure 17. Example Next Movement State.

Several seconds later, two different scenarios may occur. In the first scenario, the TSC infrastructure does not detect any more demand for the left turn, so the TSC infrastructure decides to terminate the permissive left at 34675 deci-seconds after the top of the hours and the next movement interval will be a clearance interval of 4 seconds (SY (Steady Yellow) in Figure 17). So, the SPaT message for this movement is now:

```
{ "signalGroup":2, "state-time-speed":[{ "eventState":"permissive-Movement-Allowed", "timing":{"minEndTime":34675, "maxEndTime":34675}}, { "eventState":"permissive-clearance", "timing":{"startTime":34675, "minEndTime":34715, "maxEndTime":34715}}]}
```

However, in the second scenario, if the TSC infrastructure detects additional demand for the left turn, the TSC infrastructure may decide the next movement interval is a minimum 6-second protected left turn (G (Green) in Figure 17) with a maximum 24-second duration, in which case the SPaT message for this movement is:

```
{ "signalGroup":2, "state-time-speed":[{ "eventState":"permissive-Movement-Allowed", "timing":{"minEndTime":34675, "maxEndTime":34675}}, { "eventState":"protected-Movement-Allowed", "timing":{"startTime":34675, "minEndTime":34735, "maxEndTime":34915}}]}
```

4.3.3.3.4.2 Unknown Next Movement State

MSG_SignalPhaseAndTiming Message provides a data frame, DF_MovementEventList, that contains 1 to 16 entries for the same movement at an intersection. Each entry (represented by DF_MovementEvent) represents a movement state for that movement over a period of time.

- The first entry describes the current movement state (i.e., DE_MovementPhaseState) and the time change details for the current movement (minEndTime, maxEndTime, and nextTime (if known))
- The second entry describes the movement state immediately after the current movement state terminates; and the start, minimum end, and maximum end times for the next movement state

If the next movement state, as represented by DE_MovementPhaseState, is unknown, a second entry for the movement (DF_MovementEvent) shall be sent in DF_MovementEventList as unknown.

For example, in Figure 17, lane #1 is tied to signal group #2 and currently a permissive left turn. The minimum end time for signal group 2 is currently 34675 deciseconds and the maximum end time is 35244 deciseconds from the top of the hour. At this point in time, the TSC infrastructure has not determined if the next movement state is a clearance interval or a protected left turn. So, the SPaT message for this movement would be the following:

```
{"signalGroup":2,"state-time-speed":[{"eventState":"permissive-Movement-Allowed","timing":{"minEndTime":34675,"maxEndTime":35244}},{"eventState":"unavailable","timing":{"startTime":36111,"minEndTime":36111,"maxEndTime":36111}}]}
```

4.3.3.3.4.3 No Past State

No design details provided at this time.

4.3.3.3.5 Time Change Details Design Details

The design details to fulfill the requirements for when the current signal interval state for a signal group may change follow. These requirements are defined in Section 3.3.3.3.5.

4.3.3.3.5.1 Time Change Details

The details on when the current movement state of a movement through an intersection will change is represented as timing (DF_TimeChangeDetails) and found under data frame DF_MovementEvent in MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*.

Each movement is tied to an identifier called the signalGroup (DE_SignalGroupID), which represents a collection of movements of a common type through the intersection.

Note, the signalGroup identifier is not necessarily equal to the phase number. For example, overlaps movements also have to be assigned a signalGroup identifier.

4.3.3.3.5.2 Unknown Time Change Detail

If any time change detail for a movement is required to be transmitted in the SPaT message, but the value is unknown, then that time change detail is represented by a value of 36111 for DE_TimeMark, found under data frame DF_TimeChangeDetails in MSG_SignalPhaseAndTiming Message as defined in *SAE J2735_202007*.

This CI Implementation Guide requires that the following time change details for each allowed movement be included in all SPaT messages transmitted:

- **Minimum End Time.** The earliest time when the current movement state is expected to end.
- **Maximum End Time.** The latest time when the current movement state is expected to end.

If the minimum end time or maximum end time is not known by the TSC infrastructure, then a value of unknown is used.

If the next time that the movement will be allowed is not known (See Section 4.3.3.3.6.1, Time of Next Allowed Movement), then the nextTime data element is not included in the SPaT message.

This CI Implementation Guide references the July 2020 version of SAE J2735 (*SAE J2735_202007*). The March 2016 version of SAE J2735 (*SAE J2735_201603*) uses a value of 36001 to represent unknown. The change was made to DE_TimeMark in the July 2020 version to properly address leap seconds.

4.3.3.3.5.3 Minimum End Time

The earliest time that the current and any future interval could end is represented by minEndTime (DE_TimeMark), found under the data frame DF_TimeChangeDetails in MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*.

The earliest time that a green interval could end may be constrained by the minimum green time setting, pedestrian WALK and flashing DON'T WALK times, coordination holds, or vehicle extensions. Yellow interval durations are generally fixed. The earliest time does not consider that the interval could abruptly change due to unpredictable events such as signal preemptions, or failures such as a watchdog failure or a conflict monitor.

Figure 18 is an example of minimum end times for an actuated intersection that includes Rest in Green.

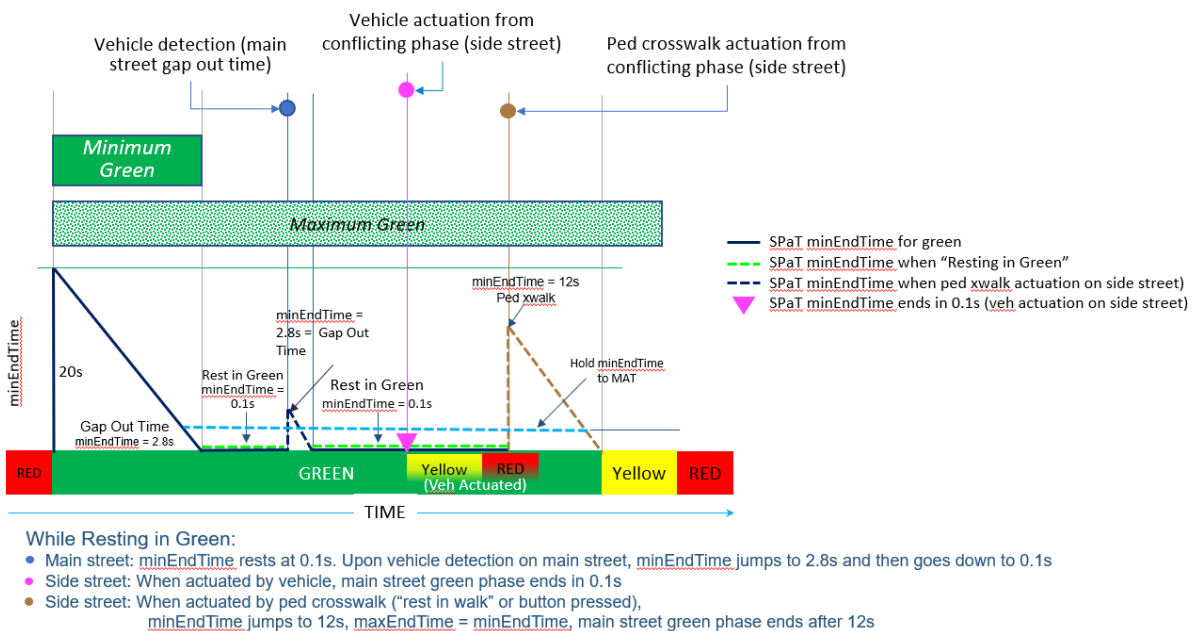


Figure 18. Example Minimum End Time, Rest in Green.

4.3.3.3.5.4 Maximum End Time

The latest time that the current and any future interval could end is represented by maxEndTime (DE_TimeMark), found under the data frame DF_TimeChangeDetails in MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*.

The latest time that an interval could end may be constrained by the maximum green time settings or coordination force-offs. When the interval duration is fixed, such as when the TSC infrastructure is operating in fixed time or the yellow interval duration, the minimum end time will equal the maximum end time.

4.3.3.3.5.5 Unknown Maximum End Time

See Section 4.3.3.3.5.2.

4.3.3.3.5.6 No Current Movement State Start Time

No design details provided at this time.

4.3.3.3.5.7 Next Movement State Start Time

MSG_SignalPhaseAndTiming Message provides a data frame, DF_MovementEventList, that contains 1 to 16 entries for the same movement at an intersection. Each entry (represented by DF_MovementEvent) represents a movement state for that movement over a period of time.

- The first entry describes the current movement state (i.e., DE_MovementPhaseState) and the time change details for the current movement (minEndTime, maxEndTime, and nextTime (if known)).
- The second entry describes the movement state immediately after the current movement state terminates; and the start, minimum end, and maximum end times for the next movement state.

The start time for the next movement state, represented by startTime (DE_TimeMark) and found under the data frame DF_TimeChangeDetails in MSG_SignalPhaseAndTiming Message in *SAE J2735_202007*, shall also be included in the second entry, even if the value is unknown. Note that the minEndTime and maxEndTime for the second entry shall also be included in the second entry, even if the value is unknown.

If the next movement state, as represented by DE_MovementPhaseState, is unknown, a second entry for the movement (DF_MovementEvent) shall be sent in DF_MovementEventList as unknown.

This CI Implementation Guide references the July 2020 version of SAE J2735 (*SAE J2735_202007*). The March 2016 version of SAE J2735 (*SAE J2735_201603*) uses a value of 36001 to represent unknown. The change was made to DE_TimeMark in the July 2020 version to properly address leap seconds.

See the example in Section 4.3.3.3.4.1, Next Movement State.

4.3.3.3.5.8 Next State Time Start Equals Current State Minimum End Time

If the TSC infrastructure knows the next movement state, the start time of the next movement state, represented by startTime (DE_TimeMark) in the second entry of data frame DF_MovementEventList, shall be the same time point as the minimum end time of the current movement state, as represented by minEndTime (DE_TimeMark) in the first entry of data frame, DF_MovementEventList.

4.3.3.3.6 Next Green Design Details

The design details to fulfill the requirements for when a movement at an intersection is next allowed to proceed (e.g., permissive or protected movement allowed) follow. These requirements are defined in Section 3.3.3.3.6.

4.3.3.3.6.1 Time of Next Allowed Movement

The next time that the current movement is allowed to move is represented by nextTime (DE_TimeMark), found under the data frame DF_TimeChangeDetails in MSG_SignalPhaseAndTiming Message in SAE J2735_202007. A movement is "allowed to move" when the signal indication for that movement is green or a flashing yellow arrow for a vehicle movement; or a "WALK" signal for a pedestrian movement; or, more precisely, the movement state, as represented by DE_MovementPhaseState, is permissive-Movement-Allowed or protected-Movement-Allowed.

Next time may be used by ECO (environmental) applications on an OBU/MU to determine when the vehicle or pedestrian is estimated to be allowed to move again. This may affect if a driver is advised to travel faster or slower to improve overall fuel consumption.

For fixed time and coordinated signals (and possibly others), next time can be estimated by the TSC infrastructure, subject to unpredictable events such as signal preemptions, or failures such as a watchdog failure or a conflict monitor. If next time cannot be estimated with a high level of confidence, a value of unknown is used, represented by a value of 36111 for DE_TimeMark.

Otherwise, a nextTime other than unknown is provided and only in the first entry (DF_MovementEvent) of DF_MovementEventList, which represents the current movement state. If the next time is unknown (or known but not with a high level of confidence), nextTime shall not be sent in DF_MovementEvent.

Note: The value of DE_TimeMark indicating undefined or unknown changed from a value of 36001 in SAE J2735_201603 to a value of 36111 in SAE J2735_202007.

For example, Figure 19 is a mid-block pedestrian crossing with a pedestrian pushbutton for the cross walk. The signal indication for the vehicle movement (signal group 1) is currently green with a minimum end time of 34675 deciseconds and the maximum end time is 35244 deciseconds from the top of the hour. At this point in time, the TSC infrastructure does not know when the movement will end, so it does not know the next time the movement will be allowed again. So, the SPaT message for this movement would be the following:

```
{ "signalGroup":1, "state-time-speed":{ "eventState":"protected-Movement-Allowed", "timing":{"minEndTime":34675, "maxEndTime":35244}}, {"eventState":"unavailable", "timing":{"startTime":36111, "minEndTime":36111, "maxEndTime":36111}}}
```

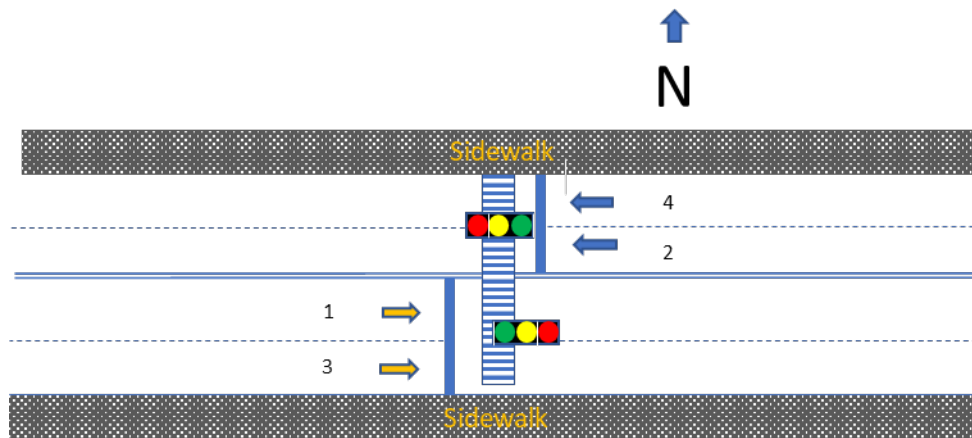


Figure 19. Example Next Time.

Several seconds later, a pedestrian depresses the pushbutton and the TSC infrastructure decides to terminate the green at 34675 deci-seconds after the top of the hour, with a clearance interval of 4 seconds. The pedestrian WALK plus flashing DON'T WALK time is 26 seconds. The next time is now

known to be 34975 deci-seconds after the top of the hour. So, the SPaT message for this movement is now the following:

```
{ "signalGroup":1, "state-time-speed":{ "eventState":"protected-Movement-Allowed", "timing":{"minEndTime":34675, "maxEndTime":34675, "nextTime":34975}}, {"eventState":"protected-clearance", "timing":{"startTime":34675, "minEndTime":34715, "maxEndTime":34715}}}
```

4.3.3.3.7 Enabled Lanes Indication

Active ('enabled') revocable lanes for an intersection are represented by the lane identifier (DE_LaneId) in enabledLanes (DF_EnabledLaneList), found under data frame DF_IntersectionState in MSG_SignalPhaseAndTiming Message as defined in *SAE J2735_202007*.

This requirement is conditional, if the intersection does not have a revocable lane defined in the MAP message for the same intersection (See 4.3.3.4.6, Revocable Lanes), OR no revocable lane is currently active ('enabled') then the data frame DF_EnabledLaneList is not transmitted in the SPaT message.

However, if the MAP message for the intersection defines a revocable lane for the intersection AND a revocable lane is currently active ('enabled'), then the data frame DF_EnabledList shall be transmitted as part of the SPaT message for the intersection.

This is an example:

```
{ "messageId":19, "value":{"intersections":{"id":{"id":173}, "revision":89, "status":"0000", "moy":19230, "timeStamp":45484, "states":{"signalGroup":2, "state-time-speed":{"eventState":"protected-Movement-Allowed", "timing":{"minEndTime":34654, "maxEndTime":35244}}}, {"signalGroup":4, "state-time-speed":{"eventState":"stop-And-Remain", "timing":{"minEndTime":34711, "maxEndTime":35301}}}}}}}
```

```
{ "messageId":19, "value":{"intersections":{"id":{"id":173}, "revision":89, "status":"0000", "moy":19230, "timeStamp":45484, "enabledLanes":5, ["states":{"signalGroup":2, "state-time-speed":{"eventState":"protected-Movement-Allowed", "timing":{"minEndTime":34654, "maxEndTime":35244}}}, {"signalGroup":4, "state-time-speed":{"eventState":"stop-And-Remain", "timing":{"minEndTime":34711, "maxEndTime":35301}}}}}}}
```

An implementation should provide a check that a SPaT message does not assert mutually exclusive enabled lanes simultaneously. Note: *NTCIP 1202 v03A* defines a table, spatEnabledLanesConcurrencyTable, which indicates which lanes may be active concurrently and serves as a check that mutually exclusive enabled lanes are not enabled simultaneously.

4.3.3.3.8 SPaT Message Accuracy

No design details provided at this time.

4.3.3.4 Roadway Geometry Data Design Details

The design details to fulfill the requirements to provide information about travel lanes follow. These requirements are defined in Section 3.3.3.4.

4.3.3.4.1 Intersection Geometry Design Details

The design details to fulfill the requirements to provide information about the lanes in and around an intersection follow. These requirements are defined in Section 3.3.3.4.1.

4.3.3.4.1.1 Intersection Geometry Information

See intersections (DF_IntersectionGeometryList) for MSG_MapData in *SAE J2735_202007*.

4.3.3.4.1.2 Intersection Geometry - Road Regulator Identifier

The road regulator identifier is represented as region (DE_RoadRegulatorID) and found under the data frame DF_IntersectionReferenceID in the MSG_MapData message in *SAE J2735_202007*.

See Section 4.3.3.3.1.2, Road Regulator Identifier, for a discussion on how road regulator identifiers may be assigned. A comment to the SAE Technical Committee responsible for maintaining *SAE J2735_202007*. The comment can be found in Annex H.1.5, DE_RoadRegulatorID.

4.3.3.4.1.3 Intersection Geometry - Intersection Identifier

The intersection reference identifier is represented as id (DE_IntersectionID) and found under the data frame DF_IntersectionReferenceID in the MSG_MapData message in *SAE J2735_202007*.

The intersection reference identifier is assigned by the IOO represented by the road regulator identifier and is unique within the road regulator identifier.

4.3.3.4.1.4 Intersection Reference Point Design Details

The design details to fulfill the requirements for the location of an intersection reference point follow. These requirements are defined in Section 3.3.3.4.1.4.

4.3.3.4.1.4.1 Intersection Reference Point - Position

Although the requirement states that the first node point should be within 327.67 meters of the intersection reference point, the preference is that the selected intersection reference point should be located such that the first node point of all lanes associated with the intersection can be represented by DE_Offset_B13 (within 40.95 meters) to allow the vehicle application to properly identify the intersection that is relevant as opposed to the other intersections that are in close proximity within the RF range.

It is customary and preferred to select a point in the middle of the intersection "crash box" or conflict area as the intersection reference point. The intersection "crash box" is defined as the inside of the crosswalk markings (or stop lines) along the outside boundary of the intersection; or between the first node of all the lanes that ingress and egress the intersection (i.e., does not include internal storage lanes).

However, the intersection reference point shall be referenced to a surveyed point, i.e., the x-, y- axis offset between the intersection reference point and a surveyed point shall be known. While it is preferred that the surveyed point be in the middle of the intersection conflict area, it is not always practical. A surveyed point can be outside the intersection conflict area, for example, signal controller cabinet or a light pole; but it shall be at the same elevation as the intersection conflict area or the z- axis offset shall be known. In such a case, an intersection reference point inside the intersection conflict area can be computed using X and Y offset distance in centimeters from the surveyed point.

Figure 20 and Figure 21 illustrates three different scenarios where the following occur:

- 1) The surveyed point is inside the intersection as the reference point, such as a manhole,
- 2) The surveyed point is outside the intersection at the traffic signal controller, and
- 3) The surveyed point at the signal controller is outside the two intersections in proximity.

It is required that the surveyed point is within 0.2 meter radial accuracy and the intersection reference point computed from the surveyed point is also within 0.2 meter accuracy.

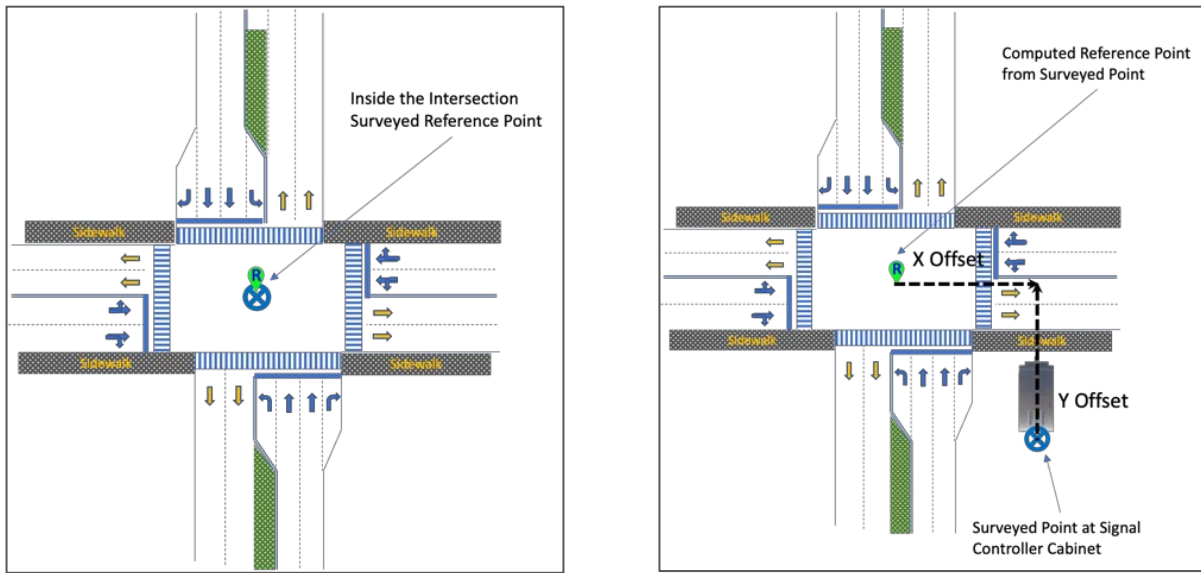


Figure 20. Intersection Reference Point Examples 1 and 2.

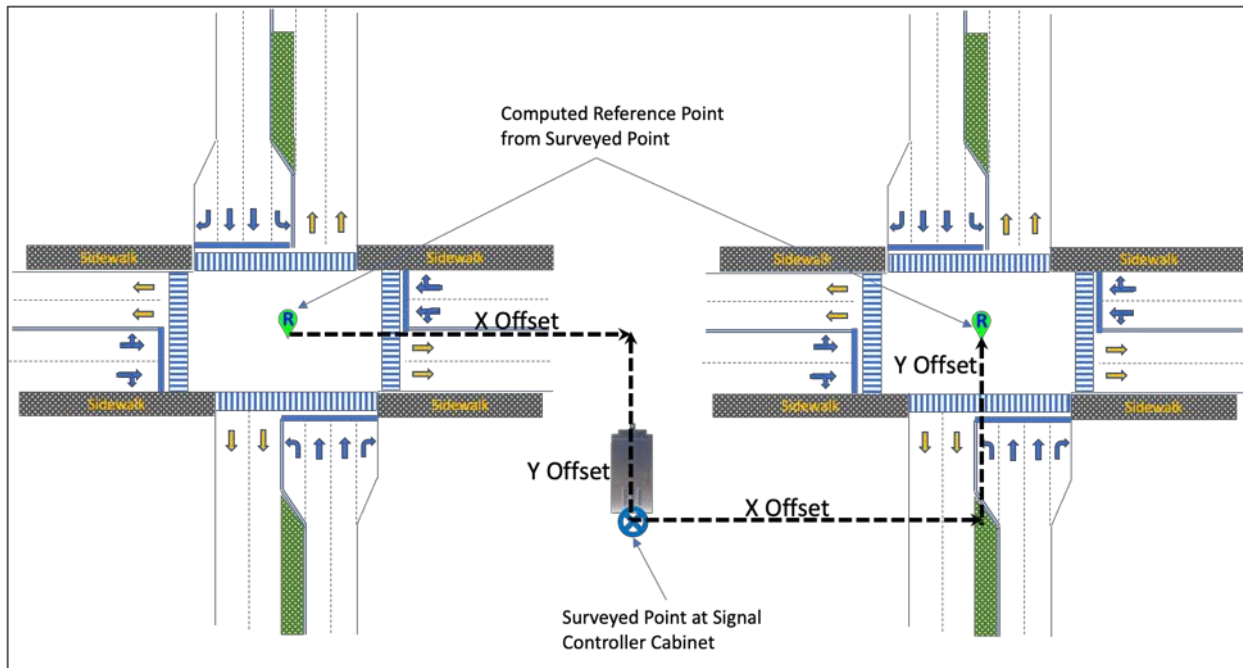


Figure 21. Intersection Reference Point Example 3.

4.3.3.4.1.4.2 Intersection Reference Point - Description

An intersection's reference point is represented as `repoint (DF_Position3D)` and found under the data frame `DF_IntersectionGeometry` in `MSG_MapData` message in *SAE J2735_202007*.

`DF_Position3D` consists of three data elements to represent the position. Latitude is represented as `lat (DE_Latitude)`, longitude is represented as `long (DE_Longitude)`, and elevation is represented as `elevation (DE_Elevation)` in `DF_Position3D`. The reference ellipsoid for `DE_Elevation` is WGS-84.

Unlike *SAE J2735_202007*, elevation is a mandatory element to conform with the CI Implementation Guide.

4.3.3.4.1.4.3 Intersection Reference Point Accuracy

The circular error of the intersection reference point location must not exceed 0.2 meters from the true location.

Because the intersection maps for connected intersections are generated using surveyed points that are aligned with the WGS 84 datum, drift of the underlying continental plate will move the intersection away from the GNSS locations of the originally surveyed node points. The North American Plate moves generally in a southwest direction at a speed of around 2.3 centimeters per year. This would mean that a node that is surveyed with centimeter accuracy could move out of that accuracy requirement within between 10 years at the most and likely sooner.

Parts of the United States also are located on the Pacific Plate, which in California moves about 5 centimeters per year to the northwest. This means that intersections west of the San Andreas Fault might have to be re-mapped more often than in other places in the country.

If the local plate movement vector is known, the MAP data could be corrected periodically and/or the intersections could be resurveyed every couple of years. By using offsets for the lane nodes, rather than absolute latitude and longitude, as required in this CI guidance, the entire intersection geometry can be corrected by simply correcting the reference point. All the other points then move to keep the same relative location from the reference point.

4.3.3.4.1.5 Default Lane Width

An intersection's default lane width is represented as `laneWidth` (`DE_LaneWidth`) and found under the data frame `DF_IntersectionGeometry` in `MSG_MapData` message in *SAE J2735_202007*. All lanes associated with the intersection are assumed to be the default lane width unless otherwise indicated (See 4.3.3.4.1.22, Node Lane Width). Lane widths are represented in centimeter units.

4.3.3.4.1.6 Lane Identifier

Each lane associated with an intersection is assigned a unique lane identifier within that intersection. The lane identifier is represented as `laneID` (`DE_LaneID`) and found under the data frame `DF_GenericLane` for intersections in `MSG_MapData` message in *SAE J2735_202007*.

The CI Committee considered several schemes for assigning lane identifiers for an intersection, but how each lane is assigned an identifier is inconsequential to an application on an OBU/MU, although there is a preference that the assignment scheme be consistent.

Schemes that have been used include assigning the first identifier for an approach to the leftmost lane, and assigning odd numbers to ingress lanes and even numbers to egress lanes, which work very well for roundabouts.

4.3.3.4.1.7 Center of Vehicle Lane Geometry

Each lane associated with an intersection is represented by node points that are located along the centerline of the lane. Each node point consists of an XY offset from a preceding node point, or the intersection's reference point. For the connected intersections, absolute positions (i.e., latitude, longitude points) are not permitted.

Read the guidance in Sections 4.3.3.4.1.11, First Node Point - Ingress Vehicle Lane Design Details to 4.3.3.4.1.23, Node Accuracy, for additional details.

For a two-way road without lane striping and permitted parking, such as a residential street, it is recommended that two overlapping lanes be defined, one in each direction. Each lane should include the "parking" lane in case there are no parked cars to indicate that "area" where cars could be parked can be used for travel. Each lane should also include the area that a vehicle can normally travel, even if it overlaps with a travel lane in the opposite direction, as shown in Figure 22.

In Figure 22, the width of lane 1 (an ingress lane) is from the sidewalk curb to a distance away from the opposite sidewalk curb, shown as a dashed line, to allow for parking on the opposite side. The width of lane 2 (an egress lane), is from the sidewalk curb on the right side to a distance away from the opposite sidewalk curb, also shown as a dashed line, to allow for parking on the opposite side. The area between the dashed lines represents an overlap of two lanes, lane 1 and lane 2. This overlapping of two lanes is represented by asserting bit 0 in `sharedWith (DE_LaneSharing)`, which can be found under the data frame `DF_LaneTypeAttributes` in the `MSG_MapData` message in *SAE J2735_202007*, to indicate overlapping lanes. See 4.3.3.4.2.2, Lane Sharing.

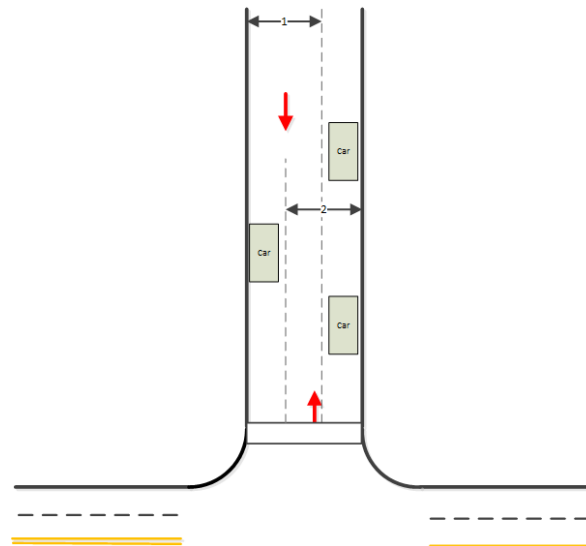


Figure 22. Center of a Vehicle Lane.

4.3.3.4.1.8 Center of Crosswalk Lane Geometry

Each crosswalk (lane) associated with an intersection is represented by node points that are located along the centerline of the crosswalk. Each node point consists of an XY offset from a preceding node point, or the intersection's reference point. For the connected intersections, absolute positions (i.e., latitude, longitude points) is not permitted.

Read the guidance in Sections 4.3.3.4.1.13 to 4.3.3.4.1.16, 4.3.3.4.1.18, and 4.3.3.4.1.20 to 4.3.3.4.1.23, for additional details.

4.3.3.4.1.9 Center of Pedestrian Landings Geometry

Each pedestrian landing associated with an intersection is represented by node points that are located along the centerline of the landing. Each node point consists of an XY offset from a preceding node point, or the intersection's reference point. For the connected intersections, absolute positions (i.e., latitude, longitude points) is not permitted.

Read the guidance in Sections 4.3.3.4.1.10, 4.3.3.4.1.13 to 4.3.3.4.1.16, and 4.3.3.4.1.19 to 4.3.3.4.1.23 for additional details.

4.3.3.4.1.10 Lane Description

See Sections 4.3.3.4.1.13 to 4.3.3.4.1.16 for additional guidance.

4.3.3.4.1.11 First Node Point - Ingress Vehicle Lane Design Details

The first node point of an ingress vehicle lane is located at the upstream edge of the stop line.

Consistent with the Connected Vehicle Pooled Fund Study's (CVPFS) *Creation of a Guidance Document for MAP Preparation*:

- In the absence of a stop line, the first node point should be placed on the upstream edge of a crosswalk marking
- In the absence of a stop line and crosswalk marking, the first node point should be placed, using engineering judgement, at the nearest point at the upstream edge of the intersection

The reason for the location of the first node point for an ingress lane is that the RLVW application needs to know where the stop line is because if the vehicle crosses the stop line (or the crosswalk marking) while the light is red, the vehicle is technically in violation, which the RLVW application tries to prevent. The RLVW application therefore needs to determine the distance from the stop line and not the distance to a location past the stop line. If the vehicle passes the stop line and stops in the crosswalk or at the edge of the intersection box while the light is red, the vehicle could get ticketed and the application design should not violate the law. Having the first node point at the location of the stop line also eliminates the need for an extra data element for the stop line location and reduces message size.

Beyond the mapped lane (i.e., downstream of the first node point), the application may have a hysteresis type design, where the lane the vehicle matched itself to is still maintained for a certain distance after crossing the first node point of the lane.

If the lane is bi-directional, such as a driveway, the first node point should follow the guidelines for the ingress direction, that is, located at the upstream edge of the stop line if present or the crosswalk marking.

Figure 23 provides several examples of locations for the first node point of lanes associated with an intersection. The first node point for most ingress lanes at this intersection are either at the upstream edge of the stop line if exists, or at the upstream edge of the crosswalk marking. Similarly, the first node point for all the egress lanes is at the downstream edge of the crosswalk, where crosswalk markings exist. However, since there is no stop line or crosswalk for lanes 2, 4, 9, or 11, engineering judgement was used to place the first node point of those lanes.

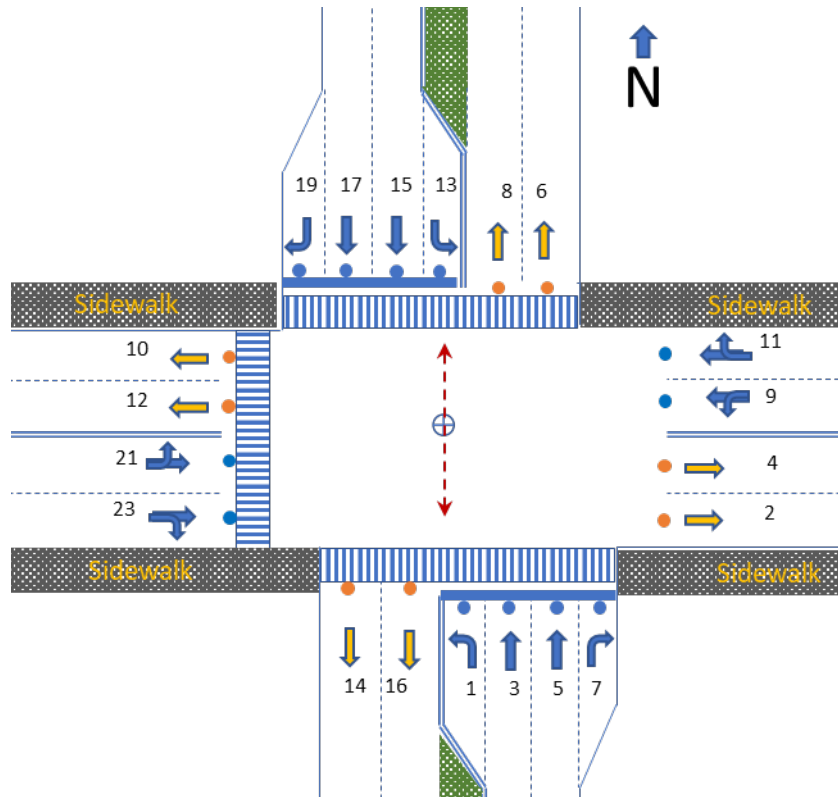


Figure 23. First Node Point.

4.3.3.4.1.12 First Node Point - Egress Vehicle Lane Design Details

The first node point of an egress vehicle lane is located at the downstream edge of the crosswalk marking.

Consistent with CVPFS's *Creation of a Guidance Document for MAP Preparation*:

- In the absence of crosswalk markings, the first node point should be determined with engineering judgement to represent the point immediately outside the intersection and any path that pedestrians might use to cross the intersection (with or without crosswalk lines). For example, curbs or cross lanes of travel could be used as references to determine the boundary of the intersection.

The reason for the location of the first node point for an egress lane is that the RLVW application needs to know if the vehicle can clear an intersection, defined as the downstream edge of the crosswalk marking of the lane the vehicle is leaving the intersection before the light turns red. If the vehicle cannot clear the intersection, the vehicle is not meeting the design goal of this CI guidance, which the RLVW application tries to prevent. The RLVW application therefore needs to determine the distance from the stop line of the ingress lane to the downstream edge of the crosswalk marking of the egress lane. If the vehicle does not clear the crosswalk marking while the light is red, the vehicle would not meet the design goal of clearing the intersection."

If a vehicle lane is reversible, the lane should be defined as two separate (revocable) lanes. So, when traveling in the ingress direction, the location of the first node point should follow the guidelines for an ingress lane, and when traveling in the egress direction, the first node point should follow the guidelines for an egress lane.

If the lane is bi-directional, such as a driveway, the first node point should follow the guidelines for the ingress direction, that is, located at the upstream edge of the stop line if present or the crosswalk marking. If there is no stop line or crosswalk marking, engineering judgement should be used.

See Figure 23 for several examples of locations for the first node point of egress lanes associated with an intersection.

Notes on egress lanes. A RLVW application only needs one point to indicate the location of the egress lane. So, an egress lane can be described with two node points 1 centimeter apart. Based on this, the minimum length of the egress lane is 1 centimeter, represented by the first node point and a second node point 1 centimeter downstream. For the purposes of RLVW application, there is no need to extend the egress lane beyond 1 centimeter.

4.3.3.4.1.13 Node Offset from Intersection Reference Point

The first node point of all lanes at or associated with an intersection is described as a node offset from the intersection's reference point. Node offsets consists of an X value, followed by a Y value and all are in 1-centimeter units. As indicated by *SAE J2735_202007*, the offset is positive to the east (X) and to the north (Y).

The node offset is represented as a choice of different data frames (node-XY1, node-XY2, node-XY3, node-XY4, node-XY5, or node-XY6, represented by DF_Node_XY_20b, DF_Node_XY_22b, DF_Node_XY_24b, DF_Node_XY_26b, DF_Node_XY_28b, and DF_Node_XY_32b, respectively) and can be found under the data frame DF_NodeOffsetPointXY in the MSG_MapData message in *SAE J2735_202007*.

The difference between the choices are the sizes of the offset data to be transmitted. Table 12 summarizes the differences between the choices, including the range of offsets supported for each choice and the number of bits required to transmit the choice. Note the number of bits required are for the X-offset and the Y-offset combined and each the same value.

Table 12. Node Offset Ranges

name	Data Frame	Range	Number of bits needed
node-XY1	DF_Node_XY_20b	+/- 5.11 meters	20
node-XY2	DF_Node_XY_22b	+/- 10.23 meters	22
node-XY3	DF_Node_XY_24b	+/- 20.47 meters	24
node-XY4	DF_Node_XY_26b	+/- 40.96 meters	26
node-XY5	DF_Node_XY_28b	+/- 81.91 meters	28
node-XY6	DF_Node_XY_32b	+/- 327.67 meters	32

The guidance is to use the smallest data frame if possible if there is a MAP message size issue, even if one lane uses different data frames (e.g., node-XY2 and node-XY4) to represent the node offsets for the same lane.

It is recommended that Universal Transverse Mercator (UTM) coordinates NOT be used because it introduces a rotation.

As shown in Figure 24, node offsets to the east are denoted by X offset and node offsets to the north by Y offset.

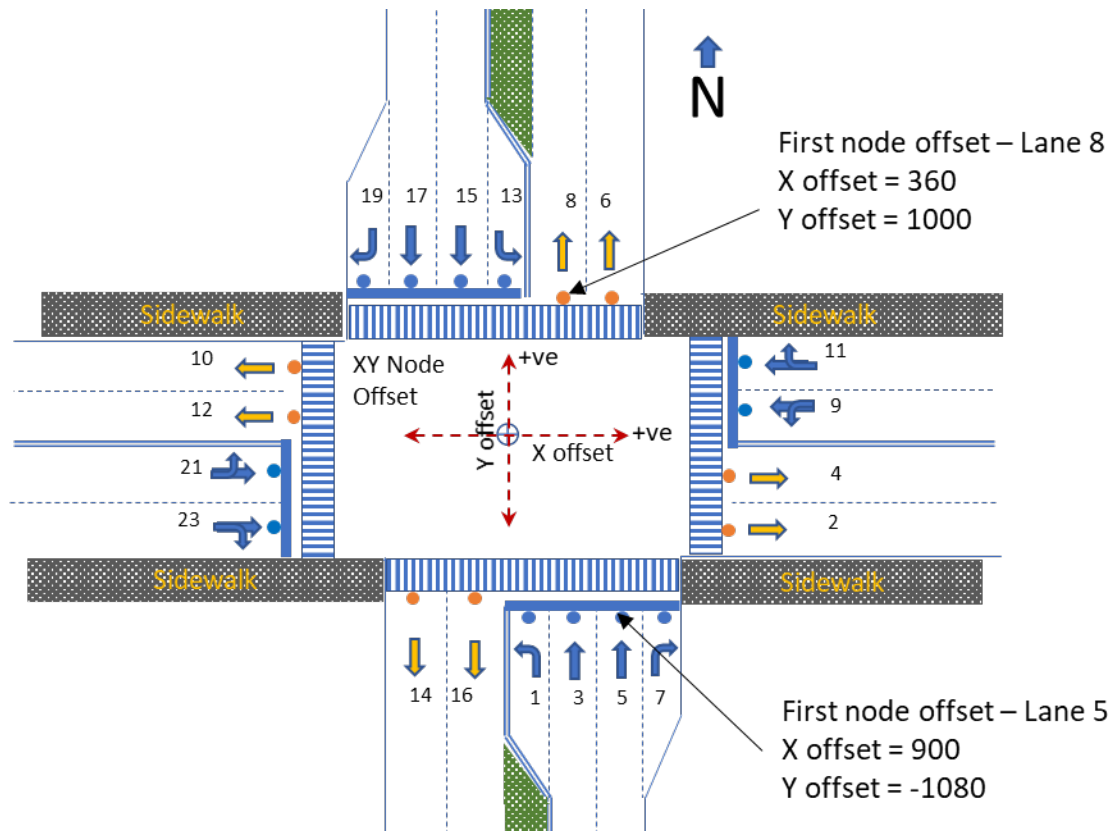


Figure 24. First Node Point Offsets.

For Figure 24, the first node point for lane id 5 and lane id 8 are the following:

```

{"laneID":5,"laneAttributes":{"..."},"nodeList":{"nodes":[{"delta":{"node-XY3":{"x":900,"y":-1080}},"delta":{"...}}]},{"laneID":8,"laneAttributes":{"..."},"nodeList":{"nodes":[{"delta":{"node-XY2":{"x":360,"y":1000}},"delta":{"...}}]}}

```

Note that since the first node point for lane id 8 is within 10.23 meters of the intersection reference point for X- and Y- offsets (the range of node-XY2), node-XY2 is used to describe the location of the first offset node point lane 8. On the other hand, the first node point for lane id 5 is outside 10.23 meters for the Y- offset, so node-XY3 is used to describe the location of the first offset node point lane 5.

4.3.3.4.1.14 Node Elevation Offset from Intersection Reference Point

The elevation of the first node point of all lanes at or associated with an intersection is described as an offset from the intersection's reference point, in one centimeter units. The elevation offset is represented as dElevation (DE_Offset-B10) and can be found under the data frame DF_NodeAttributeSetXY in the MSG_MapData message in SAE J2735_202007.

If there is no change in elevation from the intersection reference point, this data element is not sent. A positive value indicates an increase in elevation from the intersection reference point.

Figure 26 is an example of a first node point that is at a different elevation than the intersection reference point.

4.3.3.4.1.15 Offset from Previous Node

Each subsequent node point after the first node point of all lanes at or associated with an intersection is described as a node offset from the previous node point. Node offsets consists of an X value, followed by a Y value and all are in 1-centimeter units. As indicated by SAE J2735_202007, the offset is positive to the east (X) and to the north (Y).

The node offset is represented as a choice of different data frames (node-XY1, node-XY2, node-XY3, node-XY4, node-XY5, or node-XY6, represented by DF_Node_XY_20b, DF_Node_XY_22b, DF_Node_XY_24b, DF_Node_XY_26b, DF_Node_XY_28b, and DF_Node_XY_32b, respectively) and can be found under the data frame DF_NodeOffsetPointXY in the MSG_MapData message in SAE J2735_202007.

Table 12 in Section 4.3.3.4.1.13 describes the differences between the choices.

The guidance is to use the smallest data frame if possible if there is a MAP message size issue, even if one lane uses different data frames (e.g., node-XY2 and node-XY4) to represent the offsets between node points for the same lane.

Figure 25 builds on Figure 24 and shows additional node points for lanes at the intersection, including two turning bays at the same intersection. The light green lines indicate the centerline path for the vehicle in each lane.

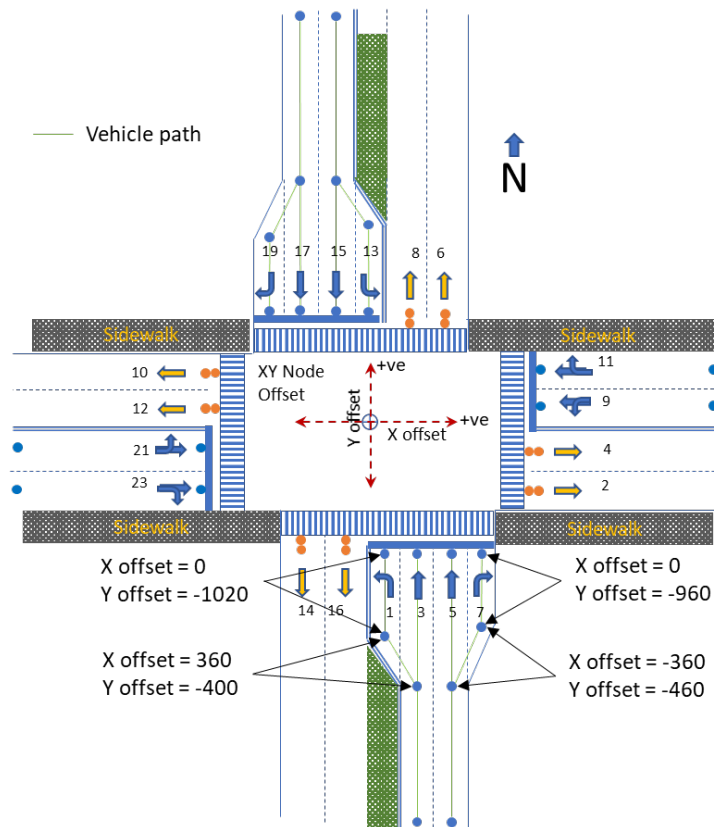


Figure 25. Node Offsets

In Figure 25, only two node points are used to define lane ids 3, 5, 15, and 17. The node points that appear between the two end node points of each lane are only used to define the last node points for lane ids 1, 7, 13, and 19. Using JSON encoding, the node points for lane ids 1, 3, 5 and 7 are the following:


```
{
  "laneID":1, "laneAttributes":{...}, "nodeList":{"nodes":[{"delta":{"node-XY3":{"x":180,"y":-1080}}}, {"delta":{"node-XY2":{"x":0,"y":-1020}}}, {"delta":{"node-XY1":{"x":360,"y":-400}}}], "laneID":3, "laneAttributes":{...}, "nodeList":{"nodes":[{"delta":{"node-XY3":{"x":540,"y":-1080}}}, {"delta":{"node-XY3":{"x":0,"y":-1840}}}], "laneID":5, "laneAttributes":{...}, "nodeList":{"nodes":[{"delta":{"node-XY3":{"x":900,"y":-1080}}}, {"delta":{"node-XY3":{"x":0,"y":-1840}}}], "laneID":7, "laneAttributes":{...}, "nodeList":{"nodes":[{"delta":{"node-XY3":{"x":1260,"y":-1080}}}, {"delta":{"node-XY2":{"x":0,"y":-960}}}, {"delta":{"node-XY1":{"x":-360,"y":-460}}]}}
```

4.3.3.4.1.16 Elevation Offset from Previous Node

The elevation offset of a node point of a lane at or associated with an intersection from a previous node point is represented as dElevation (DE_Offset-B10) and can be found under the data frame DF_NodeAttributeSetXY in the MSG_MapData message in SAE J2735_202007, in 1-centimeter units.

If there is no change in elevation from the previous node point, this data element is not sent. A positive value indicates an increase in elevation from the previous node point.

Changes in elevation are assumed to be a linear taper between the node points (it is a straight line between the two node points).

Note that SAE J2735_202007 states that changes to elevation offsets persist to subsequent nodes.

Also see Section 4.3.3.4.1.20, Maximum Distance between Nodes, for additional notes about vertical curves.

Figure 26 is a profile of a lane entering an intersection. The elevation of the first node point is located 20 centimeters higher than the elevation of the intersection reference point, and the second node point is also located 20 centimeters higher than the first node point. The third node point is at the same elevation as the second node point, while the fourth node point is 10 centimeters lower from the third node point.

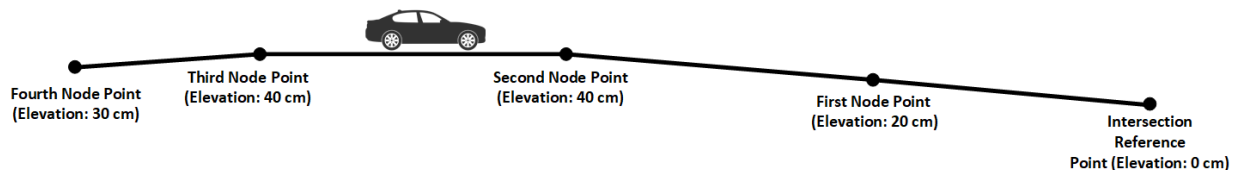


Figure 26. Elevation Offsets.

The node point representation for this lane could be (JSON encoding) the following:

```
{
  "laneID":3, "laneAttributes":{...}, "nodeList":{"nodes":[{"delta":{"node-XY3":{"x":540,"y":-1080}}, {"attributes":{"dElevation":20}}, {"delta":{"node-XY3":{"x":0,"y":-1420}}, {"attributes":{"dElevation":20}}, {"delta":{"node-XY3":{"x":0,"y":-1420}}, {"delta":{"node-XY1":{"x":0,"y":-700}}, {"attributes":{"dElevation":-10}}]}}
```

4.3.3.4.1.17 Advanced Notification - Ingress Vehicle Lane

The requirement this design detail traces to provide guidance on how far upstream should node points be provided for an ingress lane into an intersection. In addition:

- Whenever possible, the length of the ingress lanes should provide at least 10 seconds of vehicle travel in the ingress lane before the stop line. This length may be computed by multiplying the speed in mph by 4.469 to receive distance in meters. The recommendation is to use the 85th

percentile speed in the calculation or the speed limit plus 7 mph if the 85th percentile speed is not available. For 25 miles per hour, this is equivalent to an ingress lane 112 meters long.

- Ingress lanes may or may not extend beyond the egress lanes of upstream intersections. This allows an OBU application to determine where a vehicle leaves the upstream intersection without having to process the ingress lane of the downstream intersection.
- However, ingress lanes may NOT extend into or beyond the conflict area of an upstream intersection. The rationale for this constraint is a concern that extending an ingress lane into an upstream intersection may cause confusion. This driver confusion is demonstrated in the scenarios below.
 - It is recommended that if Intersection A in Figure 28 is within 10 seconds of vehicle travel in the ingress lane for Intersection B before the stop line; AND Intersection A is NOT a connected intersection, i.e., is not broadcasting MAP and SPaT messages, that the MAP content describing the intersection geometry for Intersection A be included in the RSU broadcast for Intersection B. This could either be accomplished by a separate MAP message for Intersection A being broadcast by the RSU at Intersection B (i.e., Intersection B RSU would broadcast two MAP messages one for each intersection) or could be accomplished by one MAP message that includes content describing two intersections (Intersections A and B). Including the adjoining non-CI intersection would allow the RLVW application to know not to provide warning/information before crossing the non-CI intersection.
- If Intersection A in Figure 28 is within 10 seconds of vehicle travel in the ingress lane for Intersection B before the stop line; and Intersection A IS a connected intersection, the MAP content describing the intersection geometry of Intersection A may be included in the RSU broadcast for Intersection B. This could either be accomplished by a separate MAP message for Intersection A being broadcast by the RSU at Intersection B (i.e., Intersection B RSU would broadcast two MAP messages one for each intersection) or could be accomplished by one MAP message that includes content describing two intersections (Intersections A and B). This would allow an approaching vehicle to still receive information about Intersection A in case Intersection A stops broadcasting a MAP message for any reason.

To demonstrate the driver confusion if the ingress lanes extend into or beyond an upstream intersection, two scenarios are presented below.

The following pre-conditions are assumed:

- Intersections A and B are signalized intersections
- Speed limit is 45mph
- Required MAP length (speed limit + 7mph) \cong 230m from stop point
- Distance between the intersection A and B is 150m
- RF transmission range of RSU \cong 500m

In Scenario 1, Intersections A and B in Figure 27 are signalized Connected Intersections (CI) broadcasting required messages to support in-vehicle RLVW application. Figure 27 shows operation and vehicle movements through the intersections.

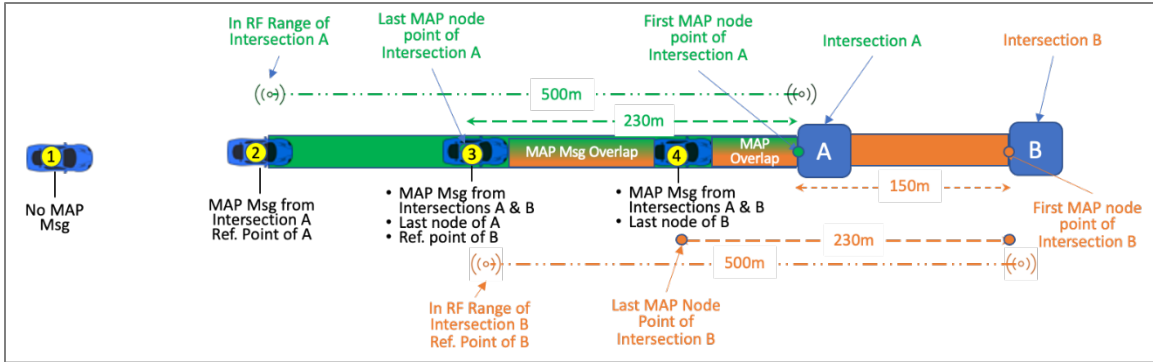


Figure 27. Overlapping Ingress Lanes - Scenario 1.

- When the approaching Connected Vehicle (CV) is at position 1, it is outside the broadcast range of RSU from intersection A, no messages are received.
- When the CV reaches position 2, it is within the broadcast range of 500m from intersection A and starts receiving messages from the intersection. At this location, the CV is 270m away from the start of mapped lanes (map is up to 230m from the intersection). The in-vehicle RLVW application can determine its lane position when the CV is in within mapped area. At this time however, the reference point (from received MAP message) is known to establish relevance of approaching intersection by the application.
- When the CV reaches position 3, it is within mapped lane definition for intersection A and within the broadcast range of intersection B. The CV now has messages from both intersections.
- When the CV is at position 4, it is within defined map of intersections A and B.
- In this scenario, the in-vehicle RLVW application would perform as intended for intersection A (being the relevant intersection) followed by the intersection B after crossing the intersection A. It is assumed that both connected intersections are operational, and broadcast required messages for the RLVW application at the time of CV traveling through the corridor.
- However, if Intersection A stops broadcasting MAP messages for any reason, such as an error condition, Scenario 2 below would occur.

In Scenario 2, Intersection A and B in Figure 28 are signalized intersections; however, Intersection A is not a Connected Intersection (CI) or not broadcasting required messages for RLVW application. Intersection B is broadcasting required messages to support in-vehicle RLVW application. Figure 28 shows operation and vehicle movements through the intersections.

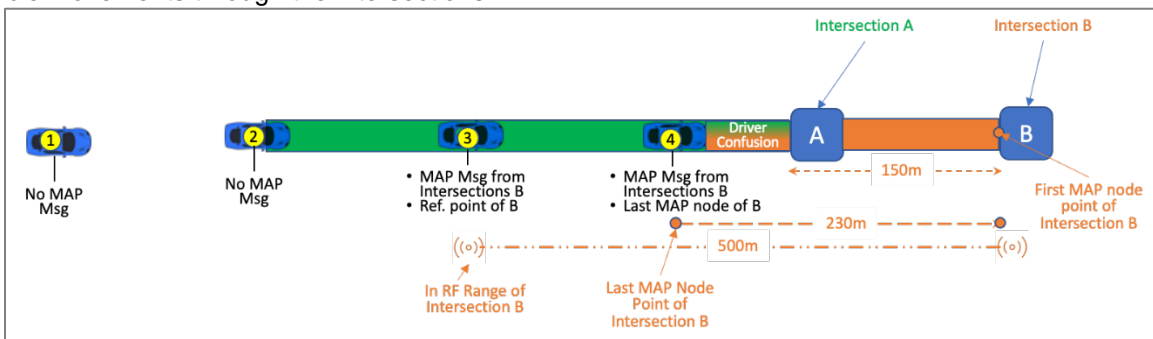


Figure 28. Overlapping Ingress Lanes - Scenario 2.

- When the approaching CV is upstream of position 3, the CV is outside the broadcast range of RSU from the intersection B and no messages are received by the CV.
- When the CV is at the position 3, it is within the broadcast range of 500m from Intersection B. From the received MAP message, for next 270 meters, the CV has the reference point location of the Intersection B, but the CV is not yet within the defined lane level map node points (maximum

230m from the intersection) for the intersection to determine its lane position to associate with SPaT for RLVW application. The in-vehicle application, however, can establish the relevance of approaching intersection based on the reference point of the intersection from the MAP message.

- When the CV is downstream of position 4, it is within mapped lane definition for the Intersection B for the in-vehicle application to determine its lane.
- When the CV is between the downstream from position 4 and before the stop point of Intersection A marked as “Driver Confusion” zone, the CV is approaching intersection A. However, the intersection relevant to the in-vehicle application is intersection B. When the CV is in the driver confusion zone and the signal phase is red or about to turn red for intersection A, the RLVW will not warn the driver since the application warning is for intersection B and not A. This may confuse the CV operator since the operator is not aware of intersection A not a CI, thinking that the RLVW system is not working.

4.3.3.4.1.18 End Nodes - Crosswalk Lane

The end nodes of a crosswalk shall be at the edge of a sidewalk curb, or a pedestrian landing. No guidance is provided on which end is the first node since the crosswalk is bi-directional.

4.3.3.4.1.19 End Nodes - Pedestrian Landing

The end nodes of a pedestrian landing shall be at the edge of the sidewalk curbs, or the crosswalk. No guidance is provided on which end is the first node since the pedestrian landing is bi-directional.

4.3.3.4.1.20 Maximum Distance between Nodes

For roadways with horizontal curves, the OBU application needs a certain amount of accuracy for lane-matching purposes. Based on calculations, the lateral accuracy of the nodes and the lane/road width must be less than 0.5 meters. To fulfill this requirement, the following formula provides the maximum distance between adjacent nodes based on the vertical curve:

$$\text{Distance between adjacent nodes [m]} = 0.058 \times \{ (\text{radius of the curve [m]} - 40\text{m}) + 12.5\text{m} \}$$

The curve geometry node points do not necessarily have to be placed equidistant to each other.

Figure 29 provides some background information related to how the above formula was derived.

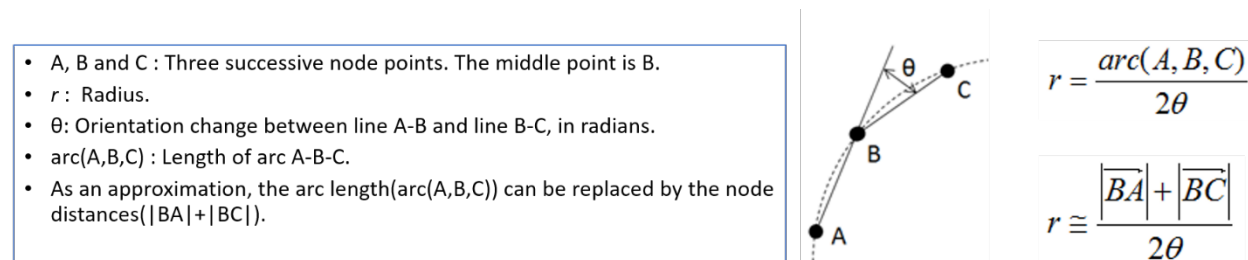


Figure 29. Maximum Distance Between Node Points.

Figure 30 is an analysis graph. The ideal distance between nodes is highlighted by a dash line in the graph. The bounded area of blue colored line and different colored square shows percentage error from ideal value.

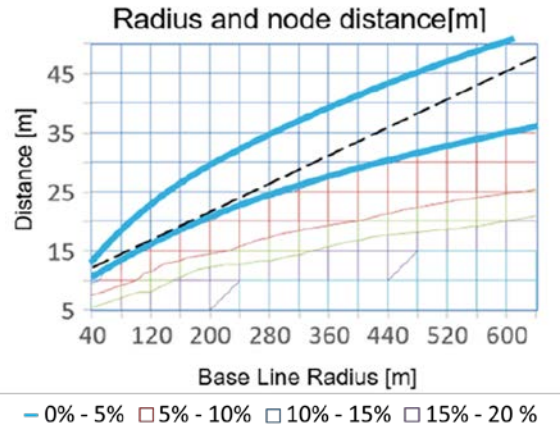


Figure 30. Radius of Curvature vs Distance Between Nodes.

Table 13 contains a suggested range of distance between node points for a curved segment.

Table 13. Radius of Curvature vs Distance Between Nodes

Radius of Curvature (m)	Distance (Range) Between Nodes (m)
< 100	15 – 20
101 to 200	22 – 30
201 to 300	25 – 35
301 to 400	30 – 38
401 to 500	32 – 45
501 to 600	35 – 52

Vertical curve information is only needed for vehicle dynamics and for deceleration. A balance is needed when adding node points between the benefits of providing vertical curve information versus the cost of the increase in message size to provide that information. A general guideline is that additional node points are not needed when the changes in elevation are 20 centimeters or less between two consecutive node points (not cumulative). Recalling that changes in elevation are assumed to be a linear taper between the node points (it is a straight line between the two node points), be aware of sudden dips in elevation, such as illustrated in Figure 31.

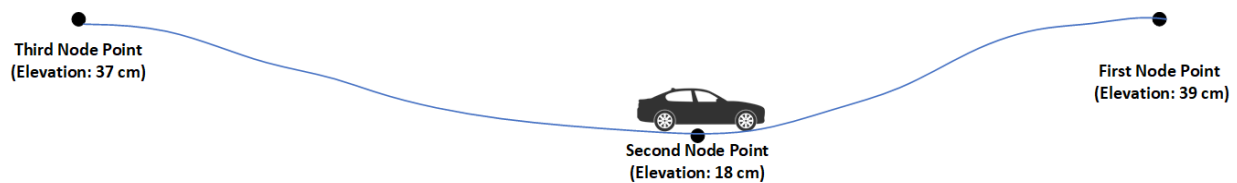


Figure 31. Vertical Curves.

No additional guidance is provided at this time for the maximum distance between nodes based on vertical curves.

4.3.3.4.1.21 Maximum Number of Nodes

It is recommended to have as few node points as possible to describe a lane to minimize the size of the MAP message, while still fulfilling requirements described in Sections 3.3.3.4.1.7 to 3.3.3.4.1.23.

4.3.3.4.1.22 Node Lane Width

The difference in the width of a lane at or associated with an intersection from the intersection's default lane width or from a previous node point is represented as `dWidth` (`DE_Offset-B10`) and can be found under the data frame `DF_NodeAttributeSetXY` in the `MSG_MapData` message in *SAE J2735_202007*, in one centimeter units.

If there is no change in the lane width from the previous node point, this data element is not sent.

If there is no change in the lane width at the first node point for the lane from the default lane width for the intersection, this data element is not sent.

A positive value indicates an increase in the lane width from the previous node point.

Changes in lane widths are assumed to be a linear taper between the node points.

For example, Figure 32 is an intersection with a default lane width of 360 centimeters. However, at the first node point of lane number 5, the lane width is 720 centimeters to the second node point, tapers down to 360 centimeters at the third node point, then remains 360 centimeters in width.

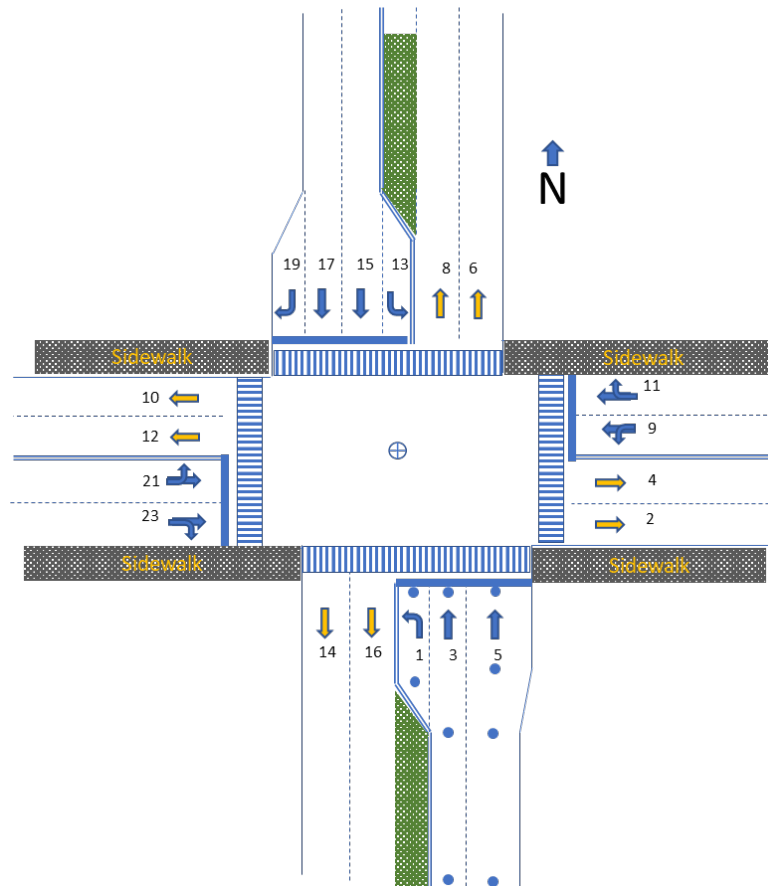


Figure 32. Lane Widths.

The node points and lane widths for lane number 5 could be (JSON encoding):

```
{"laneID":5,"laneAttributes":{...},"nodeList":{"nodes":[{"delta":{"node-XY3":{"x":1080,"y":-1080}},"attributes":{"dWidth":360}},{"delta":{"node-XY2":{"x":0,"y":-960}}},{"delta":{"node-
```

```
XY1":{"x":-180,"y":-460},"attributes":{"dWidth":-360},"delta":{"node-XY1":{"x":0,"y":-700}}}}}
```

See Figure 25 for an example on how to address tapering when a single lane becomes two lanes (or vice versa).

4.3.3.4.1.23 Node Accuracy

For a vehicle to determine what lane it is in, for the worst case of a vehicle driving along the edge line the total error cannot be more than half the vehicle width or 0.8 meters. GNSS without RTCM Corrections allows the vehicle to determine its position within 0.6 meters. This difference leaves a requirement for 0.2 meters node accuracy. If augmentation (e.g., RTCM Corrections) is provided, then $\pm 0.4/0.5$ meters may be sufficient.

The CVPFS' *Creation of a Guidance Document for MAP Preparation* document provides some guidance on how to check for node accuracy.

4.3.3.4.2 Lane Attributes

The design details to fulfill the requirements to describe the allowed use of a lane at an intersection follows. These requirements are defined in Section 3.3.3.4.2.

4.3.3.4.2.1 Direction of Travel

The allowable direction(s) of travel for a lane is represented as directionalUse (DE_LaneDirection) and can be found under the data frame DF_LaneAttributes in the MSG_MapData message in SAE J2735_202007.

DE_LaneDirection is a bit string. A value of 1 for Bit 0 indicates that the lane is an ingress lane (travel is from the last node point for a lane to the first node point of the same lane). A value of 1 for Bit 1 indicates that the lane is an egress lane (travel is from the first node point for a lane to the last node point of the same lane). A value of 0 for both Bit 0 and Bit 1 indicates no travel is allowed. A value of 1 for both Bit 0 and Bit 1 indicates travel in both directions are allowed, for example a pedestrian crosswalk.

For reversible vehicle lanes, separate lane identifiers should be assigned - one for each direction of travel, AND each lane should be identified as revocable lane (See 4.3.3.4.6, Revocable Lanes).

4.3.3.4.2.2 Lane Sharing

A shared lane is a physical lane that can be shared by different types of travelers, each with a right to use the lane. A shared lane is represented by sharedWith (DE_LaneSharing) and can be found under the data frame DF_LaneAttributes in the MSG_MapData message in SAE J2735_202007.

Common examples of shared lanes are tracked trolleys that share a vehicle lane, a bicycle lane that is shared with a vehicle lane, or a bicycle lane that is shared with a pedestrian pathway. For a connected intersection, how the lanes are coded in DE_LaneSharing depends on how the TSC infrastructure controls the different type of travelers.

For example, in Figure 33, the far left lane is defined as lane 1, and may be used by motorized vehicle and the tracked vehicles. There is no separate signalGroupID to control different types of vehicles in this lane.

In this example, there is no need to map the same physical lane twice, because there are no separate signalGroupID assigned for motorized vehicles or tracked vehicles. So, the MAP message would assign Lane id 1 to this lane as a vehicle lane type (See 4.3.3.4.2.3, Lane Type Attributes). To indicate that the lane is treated as one for motorized vehicle and tracked vehicles, the multipleLanesTreatedAsOneLane

bit is asserted to indicate "the lane object path and width details represents multiple lanes within it that are not further described;" and trackedVehicleTraffic bit is asserted to indicate "various modes and (the) type of traffic that may share this lane. The encoding for this example is as follows:

```
Bit #:          0123456789
Asserted bit:  0100000010
```



Figure 33. Example Shared Lane.

In Figure 34, the far right lane is a shared lane with motorized vehicles and tracked vehicles. However, at the intersection, there are separate signal indications (signalGroupID) for the same shared lane, one for tracked vehicles and one for motorized vehicles.

For motorized vehicles, the lane is identified as Lane 5 and has a separate signalGroupID (3), while for tracked vehicles, the lane is identified as Lane 7, but has its own signalGroupID just for tracked vehicles. In this example, Lane 5 and 7, the overlapping bit should be asserted because the lane does overlap with another defined lane (lane 5 overlaps lane 7), and are defined as separate lanes. The encoding for this example is as follows:

```
Bit #:          0123456789
Asserted bit:  1000000010
```

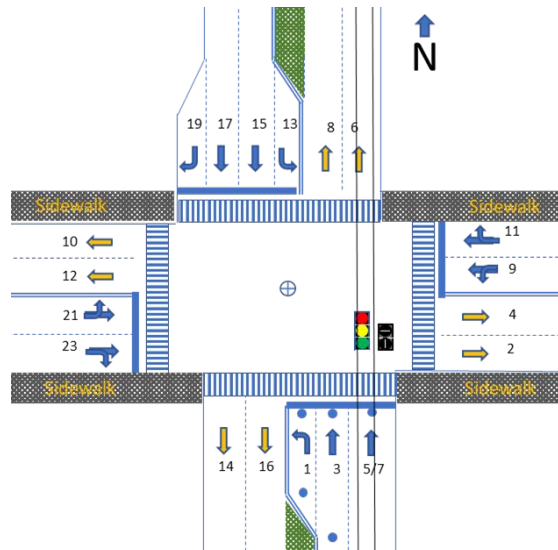


Figure 34. Shared Lane - Example 2.

As a third example, to indicate that the lane is overlapping and is also shared by taxi vehicle traffic which may stop the vehicle to pickup and drop-off customers, the overlappingLaneDescriptionProvided bit is asserted as:


```
Bit #:          0123456789
Asserted bit:  1000010000
```

4.3.3.4.2.3 Lane Type Attributes

The lane type, and its attributes, of a lane associated with an intersection is represented by laneType (DE_LaneTypeAttributes) and can be found under the data frame DF_LaneAttributes in the MSG_MapData message in *SAE J2735_202007*.

The Lane Type Attributes data frame is used to hold attribute information specific to a given lane type choice defined as the following:

```
LaneTypeAttributes ::= CHOICE {
    vehicle
    crosswalk
    bikeLane
    sidewalk
    median
    striping
    trackedVehicle
    parking
    ... }
```

Each defined lane type contains bit flags depending on its application.

The attributes of a lane type are described in the following sections (Sections 4.3.3.4.2.4 to 4.3.3.4.2.8).

4.3.3.4.2.4 Lane Attributes - Vehicle

The attributes of a vehicle lane are described by vehicle (DE_LaneAttributes-Vehicle) and can be found under the data frame (DF_LaneTypeAttributes) in the MSG_MapData message in *SAE J2735_202007*.

For example, to indicate a lane as a revocable vehicle lane but for HOV lane use only, the following bits are asserted:

```
Bit #:          01234567
Asserted bit:  10100000
```

4.3.3.4.2.5 Lane Attributes - Crosswalk

The attributes of a pedestrian crosswalk lane are described by crosswalk (DE_LaneAttributes-Crosswalk) and can be found under the data frame (DF_LaneTypeAttributes) in the MSG_MapData message in *SAE J2735_202007*.

For example, to indicate a lane as a non-revocable crosswalk lane but the path allows bicycle traffic, the following bits are asserted:

```
Bit #:          111111
                0123456789012345
Asserted bit:  0010000000000000
```

4.3.3.4.2.6 Lane Attributes - Bicycle

The attributes of a bicycle lane are described by bikeLane (DE_LaneAttributes-Bike) and can be found under the data frame (DF_LaneTypeAttributes) in the MSG_MapData message in *SAE J2735_202007*.

For example, to indicate lane as bicycle lane (not revocable) and the path allows pedestrian traffic, following bit is asserted:

```
Bit #:           111111
          0123456789012345
Asserted bit:   0100000000000000
```

4.3.3.4.2.7 Lane Attributes - Tracked Vehicles

The attributes of a tracked vehicle lane are described by trackedVehicle (DE_LaneAttributes-TrackedVehicle) and can be found under the data frame (DF_LaneTypeAttributes) in the MSG_MapData message in *SAE J2735_202007*.

For example, to indicate the lane use restricted to certain vehicle types and restricted from public use, following bit is asserted:

```
Bit #:           01234567
Asserted bit:   00000100
```

4.3.3.4.2.8 Lane Attributes - Parking

The attributes of a parking lane are described by parking (DE_LaneAttributes-Parking) and can be found under the data frame (DF_LaneTypeAttributes) in the MSG_MapData message in *SAE J2735_202007*.

For example, to indicate the revocable parking lane for head-in parking in use, following bits are asserted:

```
Bit #:           111111
          0123456789012345
Asserted bit:   1010000000000000
```

4.3.3.4.3 Lane Maneuvers

The allowed lane maneuvers for a lane at an intersection is represented by maneuvers (DE_AllowedManeuvers) and can be found under the data frame (DF_GenericLane) in the MSG_MapData message in *SAE J2735_202007*.

For example, to indicate a lane that allows straight, right turn on green and right turn on red, following bits are asserted:

```
Bit #:           11
          012345678901
Asserted bit:   101001000000
```

4.3.3.4.4 Connections Between Lanes

The design details to fulfill the requirements to describe connections between a lane entering or within an intersection; and the downstream lane at an intersection follow. These requirements are defined in Section 3.3.3.4.4.

4.3.3.4.4.1 Lane Connections

A list of permitted connections between an ingress lane and each lane a traveler may connected to. This list is represented by connectsTo (DF_ConnectsToList) and can be found under the data frame (DF_GenericLane) in the MSG_MapData message in *SAE J2735_202007*.

The DF_ConnectsToList data frame is used to provide a sequence of other defined lanes to which an ingress lane connects beyond its stop point.

For example, to indicate connection between lanes, LaneID and allowed maneuvers are specified as follows (using JSON encoding):

```
"connectsTo":[{"connectingLane":{"lane":10,"maneuver":"2400"},"signalGroup":4}]
```

Where

- "lane": "10" indicates LaneID to which the current lane connects to pass the stop point
- "maneuver":"2400" indicates following bits are asserted to allow a right turn and a stop and then proceed when safe to turn right (Right Turn On Red Allowed)

```
Bit #:          11
```

```
012345678901
```

```
Asserted bit: 001001000000
```

- "signalGroup":4 indicates the SPaT signal group that controls the movements for that connection

4.3.3.4.4.2 Connection Egress Lane

The lane identifier of the egress lane from another lane at an intersection is represented by lane (DE_LaneID) and can be found under the data frame (DF_ConnectingLane) in the MSG_MapData message in *SAE J2735_202007*.

An example of how an egress lane of a connection is represented lane is found in Section 4.3.3.4.4.1.

Although *SAE J2735_202007* allows the identifier of an egress lane to be the identifier of an ingress lane for a downstream intersection (See remoteIntersection (DF_IntersectionReferenceID) under the data frame (DF_Connection) in the MSG_MapData message, this is not recommended. By using the lane identifier of another intersection, the OBU application may need to process the MAP message for the both intersections, and assumes that the OBU receive the MAP message describing the downstream intersection. The guidance is to use the identifier of the egress lane at the intersection, then link the egress lane to the ingress lane of the downstream intersection if connection to the downstream intersection is desired. The egress lane can be defined by two node points 1 centimeter apart. See Section 4.3.3.4.1.12, First Node Point - Egress Vehicle Lane Design Details for additional guidance on egress lanes.

4.3.3.4.4.3 Connection Maneuvers

The permitted connection describes the type of maneuvers that are allowed to complete a connection between an ingress lane and an egress lane (or the next connection). The type of maneuver is represented as maneuver (DE_AllowedManeuvers) and can be found under the data frame (DF_ConnectingLane) in the MSG_MapData message in *SAE J2735_202007*.

An example snippet of a MAP message (using JSON encoding) for a permitted connection between an ingress lane and an egress lane is found in Section 4.3.3.4.4.1.

4.3.3.4.4.4 Connection Signal Group

If a permitted connection is controlled by a traffic signal indication (head), then the permitted connection is tied to an identifier called the signal group. Each signal group represents a collection of connections (or movements) that may be in an active state (e.g., permissive movement allowed or protected movement allowed) at the same time at the intersection.

The signal group is represented as signalGroup (DE_SignalGroupID) and can be found under the data frame (DF_Connection) in the MSG_MapData message in *SAE J2735_202007*.

An example of a representation of a signal group is found in Section 4.3.3.4.4.1.

For every allowed connection defined for the intersection, there should be a corresponding signal group identifier for a movement state in the SPaT message, unless the connection is not controlled by the TSC infrastructure (See 4.3.3.3.3.1, Current Movement State for a Signal Group), in which case signalGroup data element is not sent.

4.3.3.4.4.5 Include Only Permitted Connections

Sending connections that are never permitted at an intersection can cause confusion and lead to errors.

For example, an agency may have a convention that identifies four pedestrian crossings at every signalized intersection. However, if a signalized intersection only has three pedestrian crossings, the connected intersection only includes the connections for those three pedestrian crossings.

If a connected intersection contains a connection that is permitted only under certain conditions, for example during a specific time of day or during special events, the ingress lane or downstream lane shall be defined as a revocable lane (See 3.3.3.4.6, Revocable Lanes). The connection would only apply if the revocable lane is currently enabled in the SPaT message. The SPaT message also indicates if the connection is in effect or not (by indicating the current movement state for the signal group associated with that connection).

4.3.3.4.5 Speed Limit Information Design Details

The design details to fulfill the requirements to provide the speed limit for a lane at the intersection follows. These requirements are defined in 3.3.3.4.5.

4.3.3.4.5.1 Default Speed Limit

An intersection's default regulatory speed limits are represented as speedlimits (DF_SpeedLimitList) and found under the data frame DF_IntersectionGeometry in MSG_MapData message in SAE J2735_202007. All lanes associated with the intersection are assumed to use these default speed limits unless otherwise indicated.

Up to nine types of default speed limits can be defined for the intersection, along with a speed measured in 0.02 meters per second. The type of speed limit is represented by DE_SpeedLimitType and speed is represented as DE_Velocity. Minimally, vehicleMaxSpeed is provided for DE_SpeedLimitType.

For example, the following MAP message segment in JSON indicates maximum speed limit of 25 miles per hour in a school zone when children are present. The regulatory speed limit is specified using the speedLimits data frame containing type (DE_SpeedLimitType) and speed (DE_Velocity) in 0.02 meter/second units.

```
... "intersections": [{"id": {"id": 23}, "revision": 1, "refPoint": {"lat": 425207879, "long": -830473419, "elevation": 1890}, "laneWidth": 366, "speedLimits": {"type": "maxSpeedInSchoolZoneWhenChildrenArePresent", "speed": 559}}...
```

4.3.3.4.5.2 Change in Lane Speed Limit

If a lane has a speed limit that differs from the default speed limit for the intersection, the lane attribute data shall include a lane speed limit. A lane's regulatory speed limits are represented as speedlimits (DF_SpeedLimitList) and found under the data frame DF_LaneDataAttribute in MSG_MapData message in SAE J2735_202007.

If the speed limit for the lane is the same as the default speed limit for the intersection, speedlimits (DF_SpeedLimitList) is not sent.

Up to nine types of default speed limits can be defined for the lane, along with a speed measured in 0.02 meters per second. The type of speed limit is represented by DE_SpeedLimitType and speed is represented as DE_Velocity.

Any changes in the regulatory speed limits are asserted (apply) from the node point where the regulatory speed limit is first defined for the lane as ordered in the MAP message until a different speed limit is defined. For subsequent node points in the MAP message, if there is no change in the speed limit from the previous node point, speedlimits (DF_SpeedLimitList) is not sent.

For example, in Figure 35, the default speed limit for the intersection is 40 miles per hour. However, for lanes 9 and 11, the maximum speed limit is 35 miles per hour for the first 50 meters from the stop bar, then 45 miles per hour upstream from that point. The maximum speed limit for lanes 10 and 12 is also 35 miles per hour until 35 meters.

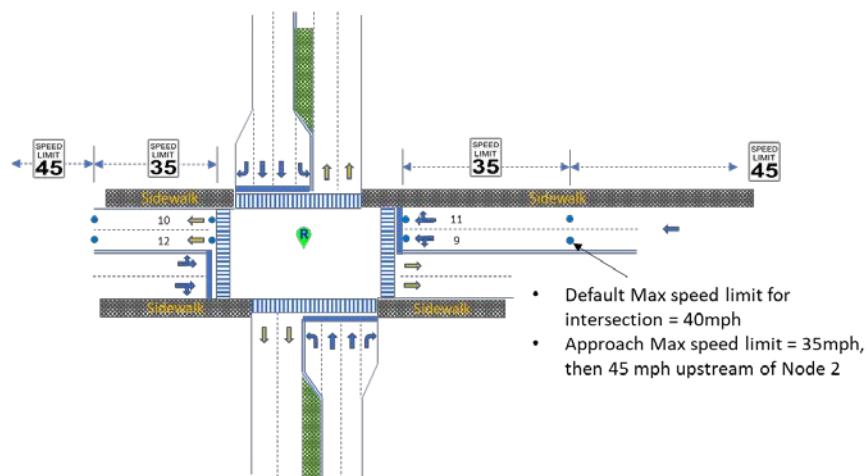


Figure 35. Changes in Lane Speed Limits.

Using JSON encoding, the node points for lane ids 9, 10, 11 and 12 are the following:

```
{
  "laneID":9,"laneAttributes":{"..."},
  "nodeList":{"nodes":[{"delta":{"node-XY3":{"x":1800,"y":180}}},
    {"attributes":{"data":[{"speedLimits":[{"speed":782,"type":"vehicleMaxSpeed"}]}]}},
    {"delta":{"node-XY5":{"x":5000,"y":0}}},
    {"attributes":{"data":{"speedLimits":[{"speed":1008,"type":"vehicleMaxSpeed"}]}]}]}},
  "laneID":10,"laneAttributes":{"..."},
  "nodeList":{"nodes":[{"delta":{"node-XY3":{"x":-1700,"y":180}}},
    {"attributes":{"data":{"speedLimits":[{"speed":782,"type":"vehicleMaxSpeed"}]}]}},
    {"delta":{"node-XY4":{"x":-3500,"y":0}}},
    {"attributes":{"data":{"speedLimits":[{"speed":1008,"type":"vehicleMaxSpeed"}]}]}]}},
  "laneID":11,"laneAttributes":{"..."},
  "nodeList":{"nodes":[{"delta":{"node-XY3":{"x":1800,"y":540}}},
    {"attributes":{"data":{"speedLimits":[{"speed":782,"type":"vehicleMaxSpeed"}]}]}},
    {"delta":{"node-XY5":{"x":5000,"y":0}}},
    {"attributes":{"data":{"speedLimits":[{"speed":1008,"type":"vehicleMaxSpeed"}]}]}]}},
  "laneID":12,"laneAttributes":{"..."},
  "nodeList":{"nodes":[{"delta":{"node-XY3":{"x":-1700,"y":180}}},
    {"attributes":{"data":{"speedLimits":[{"speed":782,"type":"vehicleMaxSpeed"}]}]}},
    {"delta":{"node-XY4":{"x":-3500,"y":0}}},
    {"attributes":{"data":{"speedLimits":[{"speed":1008,"type":"vehicleMaxSpeed"}]}]}]}]}
}
```

4.3.3.4.6 Revocable Lanes

A revocable lane is a lane that is "active" only during certain periods of time. How a revocable lane is represented is dependent on the lane type and its attributes, as represented by laneType (DE_LaneTypeAttributes) in the data frame DF_LaneAttributes (See Section 4.3.3.4.2.3). For example,

- Lane attributes for a vehicle lane are represented by vehicle (DE_LaneAttributes-Vehicle) in the data frame DF_LaneTypeAttributes
- Lane attributes for a crosswalk lane are represented by crosswalk (DE_LaneAttributes-Crosswalk) in the data frame DF_LaneTypeAttributes
- Lane attributes for a bicycle lane are represented by bikeLane (DE_LaneAttributes-Bike) in the data frame DF_LaneTypeAttributes
- Lane attributes for a tracked vehicle lane are represented by trackedVehicle (DE_LaneAttributes-TrackedVehicle) in the data frame DF_LaneTypeAttributes
- Lane attributes for a parking lane are represented by parking (DE_LaneAttributes-Parking) in the data frame DF_LaneTypeAttributes

Regardless of the lane type, a revocable lane is represented by a value of 1 for Bit 0 of the DE_LaneAttributes-xxxx, where xxxx is the type of lane.

Whether the lane for an intersection is "active" or "enabled" is defined by the Enabled Lanes indication in the SPaT message for the same intersection (See Section 4.3.3.3.7, Enabled Lanes Indication).

4.3.3.4.7 Map Message – Accuracy

No design details provided at this time.

4.3.3.4.8 Signal Timing and Roadway Geometry Synchronization

The design details to fulfill the requirements to ensure that the roadway geometry information being broadcast reflect the current operating state used to generate the signal timing data follow. These requirements are defined in Section 3.3.3.4.8.

4.3.3.4.8.1 Matching Intersection Reference Identifier

No design details provided at this time.

4.3.3.4.8.2 Matching SPaT and MAP Version

The purpose of this requirement is that the contents of the SPaT message is consistent with the MAP message being broadcasted. An example of consistency includes that the SPaT message provides state and timing information for a left turn into a lane that is defined and allowed in the MAP message.

The intent of requirement 3.3.3.4.8.2, mMatching SPaT and MAP Version is NOT that a connected intersection be able to "automatically" identify that the SPaT and MAP messages are consistent with each other. Rather, the intent of this requirement is that the IOO managing the connected intersection define policies and guidelines to prevent situations where SPaT and MAP message may conflict with each other. Policies and guidelines should address temporary situations, such as a temporary work zone; and permanent situations, such as permanent changes to the intersection configuration.

For example, the traffic signal timing plan currently being implemented by a TSC infrastructure is designed for a specific geometric configuration. However, what happens during the following scenarios:

- There are changes to the lane striping - should the connected intersection stop broadcasting the SPaT message and/or the MAP message while the striping work is underway?

- What if the egress lane for a left-turn lane movement is temporarily closed for a construction - should the MAP allowing that left turn still be broadcasted?
- After a re-striping project - should the SPaT and MAP message be checked and verified before the messages are broadcasted again? This is particularly important if the source of the SPaT and MAP messages are generated from different sources (e.g., a traffic engineering department for the SPaT message and a street construction department for the MAP message).

Be aware that some OBUs may have the capability to store MAP information, so OBU applications may reference its stored copy of the MAP data even if the MAP message is not broadcasted by the connected intersection.

This requirement is verified (tested) by inspection and/or demonstration. The method of verification can be decided by the IOO.

Note: The standards can support different methods for verifying some form of consistency between the SPaT and MAP messages. For example, *NTCIP 1202 v03A* allows a traffic signal controller to verify against a checksum of the MAP message broadcasted before the SPaT data is generated. A SPaT message can also be tied to a specific version of a MAP message, e.g., the revision counter increment (See Section 4.3.3.2.2.3, MAP Message - Revision Counter Increment).

4.3.3.5 Positioning Messages

The design details to fulfill the requirements for positioning data broadcasted by a connected intersection follow. These requirements are defined in Section 3.3.3.5.

4.3.3.5.1 Positioning Corrections

The *SAE J2735_202007* RTCMcorrections message ASN.1 representation is as follows:

```
RTCMcorrections ::= SEQUENCE {  
  msgCnt      MsgCount,  
  rev         RTCM-Revision,  
  timestamp   MinuteOfTheYear     OPTIONAL,  
  anchorPoint FullPositionVector  OPTIONAL,  
  rtcHeader   RTCMheader          OPTIONAL,  
  msgs       RTCMmessageList,  
  regional   SEQUENCE (SIZE(1..4)) OF RegionalExtension {{REGION.Reg-  
  RTCMcorrections}}                OPTIONAL,  
  ...  
}
```

A connected intersection shall increment msgCnt (DE_MsgCount) by 1 each time the RTCMmessageList contents change. Zero follows a value of 127.

A connected intersection shall use a value of rtcRev3 for rev (DE_RTCM_Revision) to indicate that RTCM corrections are per RTCM10403.3.

The OPTIONAL MinuteOfTheYear field shall not be included in the RTCMcorrections message.

The anchorPoint (DF_FullPositionVector) for a connection intersection shall include UTC, latitude, longitude, and elevation. UTC is the time at which the CI receives the corrections information included in RTCMmessage list from the reference station. The latitude, longitude, and elevation are at the location of the RTCM reference station antenna. All other fields in DF_FullPositionVector shall not be included.

Note: The UTC timestamp within FullPositionVector is within +/- 10 ms of UTC as stated in the *RSU Standard v01*. If the RTCM corrections are being generated virtually from multiple sources, the latitude, longitude, and elevation is the location of the virtual reference (usually the RSU location at CI).

Note: The location of the reference station may be used by the OBU to check the proximity of the reference station (source of the corrections). The UTC information may be used to check the age of the information. Both the time and location information may not be the same as the generation location and time information included in the security header of a signed RTCMcorrections message (i.e., it is likely different if the RSU is not the source of the corrections).

The OPTIONAL RTCMheader field shall not be included in the RTCMcorrections message.

Support for RTCM MSM 4 messages (station location message numbers 1005 or 1006, GNSS antenna and receiver location message 1033, system parameter message 1013) are mandatory and sufficient to support the RLVW application. An implementation may also provide MSM 5, 6, or 7 to support other corrections capabilities in addition to MSM 4.

Implementations shall minimally support GPS and at least one of the following constellations: GLONASS, Galileo, and BeiDou.

A connected intersection shall include only one RTCM message received from the reference station in DF_RTCMmessageList. The RSU shall broadcast an RTCMcorrections message for each message received from the reference station.

Messages 1006 (1005 if applicable), 1013, 1033 shall be combined into a single SAE J2735 RTCMcorrections broadcast (all three in the RTCMmessageList data frame in one RTCMcorrections message). MSM 4 messages (1074 plus 1084 and / or 1124) are sent together in a single RTCMcorrections broadcast (no other content is included in RTCMmessageList). If MSM 5, 6, or 7 are also being transmitted, the same approach applies; e.g., MSM 5 messages 1075 and 1085 would be sent together in the RTCMmessageList if MSM 5 is being used and GPS and GLONASS corrections are included in the J2735 RTCMcorrections message.

The regional (DF_RegionalExtension) field shall not be included in RTCMcorrections message.

4.3.3.5.2 Real-Time Kinematics Design Details

The design details to fulfill the requirements for to support real-time kinematics at a connected intersection follow. These requirements are defined in Section 3.3.3.5.2.

4.3.3.5.2.1 RSU Proximity

This section specifies the maximum distance allowed between a real-time kinematic (RTK) reference station and an RSU at any connected intersection seeking to broadcast this reference station's differential GNSS corrections formatted according to the RTCMv3.3 standard¹ (Note: the referenced link indicates v3.2, but the text is for v3.3).

The varied range of the operational conditions seen by GNSS receivers across urban and rural environments² and the unpredictability of atmospheric and space weather³ events affect the acceptable maximum distance.

¹ Radio Technical Commission for Maritime Services. [RTCM 10403.3, Differential GNSS \(Global Navigation Satellite Systems\)](#).

² National Geodetic Survey. [Minimizing Errors during GNSS Data Collection.Video Library.NGS Training and Testing Center](#).

³ NOAA / NWS Space Weather Prediction Center. [Space Weather and GPS Systems](#).

The following design requirements are recommended:

- Any RTK reference station which is to be used as a source for the CI's *SAE J2735_202007* RTCM Message shall be within 25 miles of the CI. This is based on engineering judgement, combined with references^{4,5,6} which indicate 20 km is the maximum distance to base station where centimeter-level accuracy can be obtained.
- The reference station shall be placed away from any sources of potential systematic errors, e.g., multi-path error; use the open sky definition in J2945/1 as a reference.
- It is recommended that the location of the reference station be reviewed and/or be configured by a qualified subject matter expert.
- It is recommended that the RTK reference station be located as close as possible to the connected intersection; the 25-mile requirement noted above is a maximum and locating the RTK reference station closer is preferred.

The following must be noted as the distance between the reference station and its targeted receivers grows:

- The underlying assumptions behind the RTK error correction equations physically limit the distance between the rover and reference station to approximately 25 miles.
- Relative positioning error is induced between the position of the reference station and that of the receiving rover. This distance induced relative positioning error is manufacturer and installation dependent.
- The availability of the relevant correction signals may be reduced due to differences in visible satellites between rovers and the reference station.
- Transfer of RTCM correction data from the reference station to the RSU for *SAE J2735_202007* encoding and broadcast may become more challenging and/or less reliable depending on the method of transport (LTE vs. Wire/Fiber vs. UHF radio modem).
- Transfer of RTCM correction data and the integrity of the RTK reference station need to ensure the security of this information and need to be subject to the same security as the balance of the CV environment.

It is important to note that the CI Committee also considered whether to recommend that GNSS position correction mechanisms other than RTK, such as precise point positioning (PPP) or other state-space representation (SSR) methods be broadcast by RSUs at connected intersections. The current state of the art SSR correction methods tend to use proprietary methods and message formats, proving to be even more challenging to validate than RTCM formatted correction messages. Their reported time to providing a receiver with a corrected solution under cold start conditions and following a system outage or rover disturbance also tends to be longer than conventional, single reference station-based, RTK correction methods. Finally, the business model of SSR correction providers leans on a per unit subscription model which would further increase the cost of deployment for IOOs. A single reference station within the requirement specified distance to any RSU can be used to provide RTK RTCM formatted corrections to many RSUs, only to be limited by the available communication bandwidth and the communication network architecture.

4.3.3.5.2.2 Minimum RTCM Corrections Broadcast Frequency

The design requirements are as follows:

⁴ <https://www.hindawi.com/journals/js/2019/3572605/>

⁵ <https://www.ardusimple.com/rtk-explained/>

⁶ <https://www.e-education.psu.edu/geog862/node/1845>

- MSM 4 correction broadcast rate (messages 1074, and 1084 and / or 1124) is tunable between 10 Hz (maximum rate) and 1 Hz (minimum rate).
- Messages 1005 or 1006, and 1013 and 1033 are combined into one J2735 RTCM corrections messages and sent no more frequently than once per second (1 Hz).

The assumptions and calculations that led to the above design requirements are provided in Annex Annex C, Additional Information - Positioning [Informative].

4.3.3.5.2.3 RTK/RTCM Data Trustworthiness

This requirement is fulfilled by, for example, signing the RTCM data at the point of generation, or by applying other data integrity and source authentication mechanisms to protect the RTCM between the point of generation and the point of signing.

4.3.4 Security Design Details

The design details to fulfill the security requirements for a connected intersection follow. These requirements are defined in Section 3.3.4.

4.3.4.1 Connected Intersection System Trustworthiness Design Details

The design details to fulfill the requirements for data trustworthiness for a connected intersection follow. These requirements are defined in Section 3.3.4.1.

4.3.4.1.1 SPaT Information Message Trustworthiness - RSU

A connected intersection shall fulfill requirement 3.3.4.1.1 by any vendor-specific means and shall provide documentation how this requirement is met, for example by the following:

- Firmware and software updates shall be authenticated (e.g., digitally signed) by the RSU vendor and shall be installed only by a user with administrator privilege to the RSU
- Configuration parameters that affect SPaT content shall be changeable only by an administrator authorized to do so, and over a secure connection after being authenticated as per design in Section 4.3.4.7.2.14, Access Control Policy.
- The RSU shall decide whether valid SPaT data is available at this instance or not based on at least the set frequency of the messages expected to be received from the TSC infrastructure (See Section 3.3.2.1.1.1, 3.3.2.1.1.2, and 3.3.2.1.2).

4.3.4.1.2 SPaT Information Message Trustworthiness - TSC Infrastructure

A connected intersection shall fulfill the requirement 3.3.4.1.2 by any vendor-specific means and shall provide documentation on how this requirement is met, for example such as the following:

- Firmware and software updates shall be authenticated (e.g., digitally signed) by the TSC infrastructure element's vendor, and shall be installed only by a user with administrator privilege to the TSC element.
- Configuration parameters that affect SPaT content in such a way that the SPaT information might not reflect the actual state and timing of the TSC, shall be changeable only by an administrator authorized to do so, and over a secure connection after being authenticated similar to the design details in Section 4.3.4.7.2.14, Access Control Policy.

4.3.4.1.3 MAP Data Trustworthiness

The MAP message shall be signed centrally by the MAP server. The RSU shall verify the MAP messages according to the *IEEE Std 1609.2-2016* MAP security profile in Annex D.2, upon receipt by the RSU before sending them on the V2X interface.

4.3.4.1.4 RTCM Corrections Data Trustworthiness

The (*SAE J2735_202007*) RTCM data can be obtained from the Network Transport of RTCM via Internet Protocol (NTRIP), from a Continuously Operating Reference Station (CORS), or from other sources of positioning corrections. The connected intersection shall ensure the trustworthiness of the source of this data by vendor-specific means and shall provide documentation how this requirement is met.

If the RTCM message is already signed by the source, then the RSU shall verify the RTCM message according to the *IEEE Std 1609.2-2016* RTCM security profile in Annex D.3, before sending them on the V2X interface.

See also Section 4.3.4.6.3.

4.3.4.2 Connected Intersection System Security Design Details

The design details to fulfill the requirements for network security of a connected intersection follow. These requirements are defined in Section 3.3.4.2.

4.3.4.2.1 Secure Network

The center servers (TMS, Map Data Server, and any RTCM or External control system) shall employ transport-level security in all of their interfaces.

A TMS shall implement SNMPv3 as required to support *NTCIP 1218 v01* objects.

A TMS shall implement SSH 2.0, as specified in RFC 4253.

These servers shall support TLS 1.3 as specified in *RSU Standard v1.0*, Section 4.3.5.2 Local and Back-Office Interface Security Design Details.

These servers shall not implement unsecured communication using HTTP.

NOTE: If DTLS is more appropriate than TLS and is consistent with other standards in use with the system (for example, NTCIP standards), then DTLS may be used. At the time of writing (July 2021) only DTLS 1.2 is standardized. This document permits the use of both DTLS 1.2 and, when it is standardized by IETF, DTLS 1.3.

4.3.4.2.2 Assurance of Connection to Correct Network

The RSU shall ensure it is connected to the correct TMS and the TSC infrastructure by implementing the design specified in Sections 4.3.4.6.1, Interface between RSU and TMS and 4.3.4.6.4, Interface between an RSU and the TSC Infrastructure, respectively.

This requirement does not apply to the TMS (and MAP server if applicable), since they have assurance to be connected to the correct network by being physically part of the IOO network.

4.3.4.3 Verification of Connected Intersection System Security Design Details

The design details to fulfill the requirements to provide verification of a connected intersection's compliance to system security requirements follow. These requirements are defined in Section 3.3.4.3.

4.3.4.3.1 Security Compliance Assessment

To verify that the security compliance assessment documentation is complete and correct, the security compliance assessment documentation is inspected, and this may be accomplished by self-declaration. The compliance assessment documentation should include the following:

- All known attack methodologies and mitigations that might lead to the RSU transmitting incorrect SPaTs, and their mitigation, including:
- All known attack methodologies that might lead to the TSC infrastructure outputting incorrect SPaT information message, and their mitigation
- All known attack methodologies and mitigations that might lead to the RSU transmitting incorrect MAPs, and their mitigation
- All known attack methodologies and mitigations that might lead to the RSU transmitting incorrect positioning corrections (e.g., RTCM corrections)

NOTE: These security documentation requirements are anticipated to change over time. While self-declaration is currently acceptable, the security compliance assessment documentation requirements themselves may change over time (for example, becoming more specific), and self-declaration may be replaced by a certification process involving an external party. As such, the IOO shall identify which version of the CI Implementation Guide the security compliance assessment documentation conforms with. Doing so may mitigate deployment delays associated with compliance security assessment documentation that may not conform to later requirements. Annex E.2 provides an example process of how an IOO may prepare its security compliance assessment documentation.

The document is expected to cover the following areas:

- Auditing of devices for detection and treatment of security incidents
- SPaT message trustworthiness of Sections 4.3.4.1.1 and 4.3.4.1.2
- MAP data trustworthiness of Section 4.3.4.1.3
- RTCM data trustworthiness of Section 4.3.4.1.4
- Protection against TSC reconfiguration from the RSU, Section 4.3.4.6.4.3
- MAP Data Integrity, Section 4.3.4.6.6.2
- TMS Device protection, Section 4.3.4.7.1.2
- TSC Infrastructure security standards, Section 4.3.4.4.5
- Operational Logging- TSC Infrastructure, Section 4.3.4.7.2.9
- Operational Logging – TMS, Section 4.3.4.7.2.8
- RSU Protection, Section 4.3.4.7.1.1

4.3.4.3.2 Point of Certification

Requirement 3.3.4.3.2 is verified by inspection.

4.3.4.4 Certificate Issuing Design Details

The design details to fulfill the requirements for obtaining *IEEE Std 1609.2-2016* certificates follow. These requirements are defined in Section 3.3.4.4.

4.3.4.4.1 Certificate Issuance

While third party assessment is expected in the future, currently the organization responsible for signing SPaT and MAP messages shall provide a self-declaration of having met the security requirements contained in this document to the SCMS provider they have selected. The SCMS provider shall then issue certificates.

It is expected that in the future, the requirement will be to obtain one or more certifications from third parties which will need to be submitted in addition to self-declarations for items not covered in those certifications.

4.3.4.4.2 Certificate Nonissuance

It is the responsibility of the IOO to ensure that their system initially complies with the security requirements and continues to do so in operation. The IOO asserts compliance to the SCMS provider by providing a self-declaration that the CI meets these requirements. If the IOO discovers that parts of the system no longer comply with the security requirements, the IOO is required to notify the SCMS provider. Devices affected by this non-compliance are no longer eligible for *IEEE Std 1609.2-2016* certificates and the SCMS provider is expected to no longer issue *IEEE Std 1609.2-2016* certificates to those devices until the non-compliance is addressed and the SCMS provider is notified that those parts of the system are now back in compliance.

NOTE: In the future, it is expected that self-declaration will not be acceptable on its own, and that the IOO will be required to acquire certifications from one or more third parties and present those certifications to the SCMS in order to receive *IEEE Std 1609.2-2016* certificates. Deployers are expected have access to and comply with the most recent version of these security requirements.

4.3.4.4.3 CI Operation Security Practices

The security policy shall document both the policies for the computer equipment and the human operators of that equipment. The policy shall include information on how personnel are trained for security operations and any audits or periodic reviews of policies and procedures that will be performed.

4.3.4.4.4 RSU Security Standards

The RSU shall comply with *RSU Standard v1.0*, Section 4.3.5.12 Secure Management of X.509 Credentials for TLS Design Details.

4.3.4.4.5 TSC Infrastructure Security Standards

A TSC infrastructure shall fulfill requirement 3.3.4.4.5 via IOO-specific means and shall provide documentation about the security standards met.

4.3.4.5 Security Against Cyber Attack Design Details

The design details to fulfill the requirements for security against cyber attacks follow. These requirements are defined in Section 3.3.4.5.

4.3.4.5.1 Cyber-Attack Recovery Plan

A cyber-attack recovery plan recognizes and incorporates the principles identified in the *CIS Controls Implementation Guide for Industrial Control Systems*. In addition, cyber-attack recovery plans require frequent updates to ensure that the plan remains effective, as new attacks are developed and launched.

A connected intersection shall fulfill requirement 3.3.4.5.1 via IOO-specific means based on principles outlined in the *CIS Controls Implementation Guide for Industrial Control Systems*, Control 10 – Data Recovery Capabilities and Control 19 – Incident Response and Management.

4.3.4.5.2 Cyber-Attack Robustness

To maintain robustness, a connected intersection (and/or its operators) requires continuous vulnerability management via provisions in *CIS Controls Implementation Guide for Industrial Control Systems*.

A connected intersection shall fulfill requirement 3.3.4.5.2 via IOO-specific means based on principles outlined in the *CIS Controls Implementation Guide for Industrial Control Systems*, Control 3- Continuous Vulnerability Management, Control 6 – Maintenance, Monitoring, and Analysis of Audit Logs, and Control 8 – Malware Defenses.

4.3.4.5.3 Network Protection

A connected intersection system shall implement network monitoring with continuous vulnerability management according to requirement of 3.3.4.5.3 via IOO-specific means based on principles outlined in the *CIS Controls Implementation Guide for Industrial Control Systems*, Control, Control 11- Secure Configurations for Network Devices such as Firewalls, Routers, and Switches, and Control 12 – Boundary Defense.

For example, the firewall policy should not accept incoming connections to the RSU from outside the network, and only allow the RSU to initiate connections to SCMS domains in which it is of the SCMS it is enrolled in.

4.3.4.6 Data Flow: Communications and Interface Security Design Details

The design details to fulfill the requirements for the security of data exchanges across each interface in the CI system follow. These requirements are defined in Section 3.3.4.6.

4.3.4.6.1 Interface between RSU and TMS

The design details to fulfill the requirements for the security of data exchanges between an RSU and a TMS follow. These requirements are defined in Section 3.3.4.6.1.

4.3.4.6.1.1 General RSU-TMS Interface Design Details

The design details to fulfill the general requirements for the security of data exchanges between an RSU and a TMS follow. These requirements are defined in Section 3.3.4.6.1.1.

SNMPv3 is an application layer protocol that runs on top of security protocols like TLS or SSH.

4.3.4.6.1.1.1 Secure Transport of Use of SNMPv3

When using SNMPv3, the RSU shall use the Transport Layer Security Transport Model, as defined by RFC 6353 or later.

NOTE - RFC 6353 is based on (D)TLS 1.2 and there are technical ambiguities as to how it should be paired with (D)TLS 1.3. While RFC 6353 is expected to be updated to address these issues, RSU implementations prior to the release of this update are allowed to use (D)TLS 1.2 for SNMPv3 operations.

The RSU shall comply with *RSU Standard v1.0*, Section 4.3.5.11.1.1 Secure Administration - SNMPv3 Design Details.

4.3.4.6.1.1.2 Use of (D)TLS for other Management Protocols

The RSU shall use TLS 1.3, as specified in *RSU Standard v1.0*, Section 4.3.5.2 Local and Back-Office Interface Security Design Details, for interfaces implementing HTTPS or WebSocket protocols when the RSU is acting as a TLS server. For example, this would apply to a REST API implemented by the RSU.

The RSU may also support DTLS 1.3.

The RSU shall not implement unsecured communication using HTTP.

4.3.4.6.1.1.3 Use of SSH

The RSU shall implement SSH 2.0, as specified in *RFC 4253*.

NOTE: In order to fully support *NTCIP 1218*, the RSU has to implement SFTP (or SCP) as a mechanism to transfer files to and from the RSU. SFTP and SCP both use SSH 2.0 as the underlying secure transport protocol.

The RSU may limit SSH 2.0 protocol access to SFTP (or SCP) only and prevent remote command line access via SSH.

The RSU shall comply with *RSU Standard v01*, Section 4.3.5.11.1.3 Secure Administration – SSH Design Details.

4.3.4.6.1.2 (D)TLS Certificate Design Details

The design details to fulfill the requirements for TLS and DTLS certificates (X.509 format) for an RSU follow. These requirements are defined in Section 3.3.4.6.1.2.

4.3.4.6.1.2.1 (D)TLS Authentication - Installation

If the RSU acts as a TLS or DTLS server, the RSU shall support installation of a chain of trust for validation of client certificates via a secure, vendor-specific mechanism, as defined in *RSU Standard v1.0*, Section 4.3.5.12.1 Secure Interface for X.509 Credentials for TLS Design Details. For additional information see also Section 4.3.4.6.1.2.3, RSU Certificate Security in this document.

If the RSU acts as a TLS or DTLS server, the RSU shall support installation or configuration of an IOO-specific naming pattern for certificates (see 4.4.4.6.1.2.2).

4.3.4.6.1.2.2 (D)TLS Authentication - Rejection

When the RSU acts as a TLS or DTLS server, the RSU is required to reject connection attempts from clients presenting an invalid client certificate.

To do so, the RSU currently validates a client's certificate based on the following minimum criteria:

- a) The current date is within the client certificate's validity time period, and
- b) The client certificate has been signed by a CA which is listed as part of an installed chain of trust, and
- c) The client certificate is contained within the certificate "allow list" (as indicated in *RSU Standard v1.0*, Sections 4.3.5.9.1 Assurance of Correct Initial Network Connection Design Details, and 4.3.5.9.2 Assurance of Continued Correct Network Connection Design Details).

However, the "allow-list" does not accommodate the frequently changing nature of client certificates. Therefore, the allow-list provision is deprecated (not recommended for new implementations). New implementations should use, and existing implementations should migrate to, a SubjectAltName design provision, as follows:

Replacement c) provision: The SubjectAltName field in the client certificate matches an IOO-specific naming pattern (e.g., to distinguish between certs from the same root certificate authority but for different IOOs). The naming pattern shall support wildcards which can be used to allow all names with a certain suffix, e.g., "* .cityofnyc.gov."

NOTE: The alternate design using SubjectAltName and naming pattern is preferred, and the "allow list" practice is deprecated and efforts are underway to incorporate this change in *RSU Standard v1.0*.

NOTE 2: "Allow-lists" still exist for CA certificates by virtue of the CA certificates being part of a chain of trust. However, CA certificates roll over much less frequently.

4.3.4.6.1.2.3 RSU Certificate Security

If the RSU acts as a TLS or DTLS server, the RSU shall support installation of a private key and corresponding certificate containing the public key by an administrator. The RSU shall use those to identify the server to CI components it connects to.

The RSU server certificate shall have the X.509 standard format and shall be signed by a certificate authority (CA) trusted by the IOO.

NOTE: The IOO may use a commercial CA service or operate its own public key infrastructure.

The RSU shall support installation of at least one chain of trust, containing at least one trusted CA certificate, by an administrator. A chain of trust may also contain one or more intermediate CA certificates and a trust anchor certificate (aka root certificate). In the chain of trust the lowest CA's certificate has been signed by the next higher CA, chaining all the way to the top CA, also known as the root CA.

If the RSU acts as a TLS or DTLS server, the RSU shall use the methods of Section 4.3.4.6.1.2.2, (D)TLS Authentication - Rejection, to validate client certificates.

If the RSU acts as a TLS or DTLS client, the RSU shall use this chain of trust to validate server certificates of TLS servers that it connects to.

4.3.4.6.1.2.4 RSU Client Certificate Security

The RSU shall support the configuration of a SubjectAltName pattern which is used to validate TLS client certificates (see also section 4.3.4.6.1.2.2, (D)TLS Authentication - Rejection).

The IOO shall have assurance that the SubjectAltName entries in each of their issued certificates are unique under the CA that issued the certificates.

The RSU shall provide an interface to allow an administrator to install trust anchors for X.509 certificates. The RSU shall support trust anchor installation by one or more of the following methods and shall not support other methods for installing trust anchors:

- a) A logged in administrator, using an administrator password, installing the trust anchor interactively (see NOTE 1)
- b) An authenticated SNMPv3 operation
- c) An automated operation involving signatures that chain back to an existing trust anchor.
- d) Via an authenticated operation using (D)TLS 1.3 with a protocol other than SNMPv3, e.g., HTTPS (i.e., REST API) or WebSocket

NOTE 1: (a) May only be used to install an initial chain of trust, when no other is installed. After that, a method (b), (c) or (d) must be used, i.e., a (D)TLS-protected protocol will have to be used to update.

NOTE 2: The above requirements are due to the fact that installation of trust anchors is a very sensitive operation. These requirements are expected to be updated in future versions of this document and deployments may need to adhere to these new requirements in order to continue to be issued new certificates.

NOTE 3: RSU (D)TLS server certificates as well as (D)TLS client certificates are expected to be relatively short-lived, having a validity period on the order of one week or two. With this approach it is possible to omit usage of CRLs and/or Online Certificate Status Protocol (OCSP) calls to a CA server in order to

check the revocation status of individual certificates, while still achieving a reasonable level of security protection.

4.3.4.6.2 Interface between RSU and SCMS

The RSU shall comply with *RSU Standard v1.0*, Section 4.3.5.10.3.1 SCMS Connectivity Design - CAMP.

Alternatively (and preferred going forward, for new implementations), the RSU shall comply with *RSU Standard v1.0*, Section 4.3.5.10.3.2 SCMS Connectivity Design – IEEE Std 1609.2.1.

The CI backend network shall require secure domain-name server lookup for IP addresses obtained from outside their network, i.e., DNSSEC (according to RFC 4033, 4034 and 4035).

4.3.4.6.3 Interface between an RSU and the OBU/MU

The RSU shall ensure that the messages it sends across the RSU to OBU interface are secured as follows:

- SPaT messages are signed as per *IEEE Std 1609.2-2016* and the SPaT security profile of Annex D.1
- MAP messages are signed as per *IEEE Std 1609.2-2016* and the MAP security profile of Annex D.2
- RTCM messages are signed as per *IEEE Std 1609.2-2016* and the RTCM security profile of Annex D.3

SPaT messages are signed by the RSU. RTCM messages may be signed by the RSU or the RTCM source. MAP messages are signed by the MAP data server.

The RSU shall comply with *RSU Standard v1.0*, Section 4.3.5.1.1 Security - Sending V2X Messages Design Details.

The RSU shall comply with *RSU Standard v1.0*, Section 4.3.5.1.2 Security - Receiving and Forwarding V2X Messages Design Details.

4.3.4.6.4 Interface between an RSU and the TSC Infrastructure

The design details to fulfill the requirements for the security of data exchanges between an RSU and a TSC infrastructure follow. These requirements are defined in Section 3.3.4.6.4.

4.3.4.6.4.1 Use of Secure Transport Protocol

The RSU shall implement the *NTCIP 1202 v03A* interface as specified in *RSU Standard v1.0*, Section 4.3.2.14.2 SPaT Processing Design Details - NTCIP 1202.

The RSU shall secure this interface, and any SNMPv3 interface, using SNMPv3 over TLS 1.3 or DTLS 1.3 (TLS 1.2 or DTLS 1.2 until version 1.3 is available for use with SNMP) with mutual authentication, with the RSU acting as a (D)TLS server.

The TSC infrastructure shall use this interface to establish a secure connection with the RSU and send SPaT information to the RSU.

4.3.4.6.4.2 Use of (D)TLS Protocol

The TSC infrastructure shall use its client certificate to authenticate itself to the RSU via SNMPv3 over TLS 1.2.

The TSC infrastructure shall support a vendor-specific and secure mechanism to install a client certificate along with a private key.

The TSC infrastructure shall support a vendor-specific and secure mechanism to install a chain of trust for validation of the RSU's (D)TLS server certificate.

The (D)TLS certificate design details specified in Section 4.3.4.6.1.2, (D)TLS Certificate Design Details, apply to the interface between the TSC infrastructure and the RSU.

4.3.4.6.4.3 Protection against TSC Infrastructure Reconfiguration from the RSU

The connected intersection shall fulfil the requirement of 3.3.4.6.4.3 by any vendor-specific means and shall provide documentation how this requirement is met.

4.3.4.6.4.4 Validation of Forwarded V2X Messages

If the RSU is configured to forward the Basic Safety Messages it receives from OBUs/MUs over the V2X interface to the TSC infrastructure, the RSU shall validate these messages in conformance with the relevant design in the *RSU Standard v1.0*, Section 4.3.5.1.2 Security - Receiving and Forwarding Messages Design Details.

4.3.4.6.5 Interface between the TMS and the TSC Infrastructure

The communication on this interface shall be secured using mutual authentication of both TMS and TSC infrastructure identities, and at least integrity protection of all data exchanged. It is preferred to use SNMPv3 over TLS or DTLS 1.3 or, if not yet available, over TLS or DTLS 1.2.

4.3.4.6.6 Interface between the MAP Server and the TMS

The design details to fulfill the requirements for the security of data exchanges between a MAP Server and a TMS follow. These requirements are defined in Section 3.3.4.6.6.

4.3.4.6.6.1 Secure Connection to MAP Server

A TMS shall establish a connection to the MAP server that supports transport layer security via the TLS 1.3 protocol, with certificate-based mutual authentication and integrity and encryption of data exchanged.

4.3.4.6.6.2 MAP Data Integrity

A connected intersection shall fulfil the requirement of 3.3.6.6.2 by any vendor-specific means and shall provide documentation how this requirement is met.

4.3.4.6.6.3 MAP Data Signature

The signature generated by the MAP server for the MAP message sent to the TMS shall follow the MAP message security profile in Annex D.2, Security Profile for MAP Messages.

Note: the "generation time" is the time instance that the MAP message is signed.

4.3.4.6.7 Interface between MAP Server and the SCMS

The MAP server shall be able to periodically connect to a SCMS Registration Authority server configured in the MAP server, in order to obtain *IEEE Std 1609.2-2016* certificates with appropriate permissions to sign MAP messages.

4.3.4.7 Correct Operations Design Details

The design details to fulfill requirements to provide correct operations for a connected intersection follow. These requirements are defined in Section 3.3.4.7.

4.3.4.7.1 Device Protection Design Details

The design details to fulfill the requirements to protect field components of a connected intersection from network attacks follow. These requirements are defined in Section 3.3.4.7.1.

4.3.4.7.1.1 RSU Protection

The RSU shall comply with *RSU Standard v1.0*, Section 4.3.5.8 RSU Operating System Security Design Details. This includes support for disabling unused applications and services (see Section 4.3.5.8.1 RSU OS Applications and Services Design Details therein). This includes temporarily blocking / closing unused IP ports (see Section 4.3.5.8.2 RSU OS Ports and Protocols Design Details therein).

If the RSU provides additional protections, for example blocking individual source IP addresses as described in Section 3.3.4.7.1.1, this shall be documented in the security documentation. See Section 4.3.4.3.1 for an overview of security documentation that the connected intersection operator is required to prepare.

NOTE: If the RSU blocks individual source IP addresses, care should be taken that an attacker cannot use this mechanism to trick the RSU into blocking communications from the TSC infrastructure or from the TMS.

4.3.4.7.1.2 Device Protection

A connected intersection shall fulfil the requirement of 3.3.4.7.1.2 by any vendor-specific means and shall provide documentation how this requirement is met, for example the TMS employs malware and intrusion detection and protection, IP-level firewall (e.g., iptables) supporting at a minimum closing of all unused ports by default and opening the *NTCIP 1218 v01* port for outgoing connections only.

See 4.3.4.3.1 for an overview of security documentation that the connected intersection operator is required to prepare.

4.3.4.7.2 Secure Administration of RSU

The design details to fulfill the requirements to provide secure administration of an RSU follow. These requirements are defined in Section 3.3.4.7.2.

4.3.4.7.2.1 Secure RSU Administration User Interface

The RSU shall comply with *RSU Standard v1.0*, Section 4.3.5.11 Secure Administration Design Details.

4.3.4.7.2.2 Password Change Prompt

If the RSU provides a web-based administration user interface, the RSU shall comply with *RSU Standard v1.0*, Section 4.3.5.11.1.2 Secure Administration - Web-Based Access Design Details.

Note: The referenced section requires that the password be changed from the default password.

If the RSU provides an SSH-based administration command line interface, the RSU shall comply with *RSU Standard v1.0*, Section 4.3.5.11.1.3 Secure Administration – SSH Design Details.

Note: The referenced section requires that the password be changed from the default password.

4.3.4.7.2.3 Remote Restart

The RSU shall comply with *RSU Standard v1.0*, Section 4.2.3 Requirements Traceability Matrix (RTM) Table, FR ID 3.3.2.1.2 RSU Restarts.

4.3.4.7.2.4 Log Restarts

The RSU shall comply with *RSU Standard v1.0*, Section 4.3.2.3 Log Restarts Design Details.

4.3.4.7.2.5 Factory Default

The RSU shall comply with *RSU Standard v1.0*, Section 4.3.2.2 Factory Default Design Details.

4.3.4.7.2.6 Protection against Tampering

The RSU shall comply with *RSU Standard v1.0*, Section 4.3.5.6.1 Tamper Evident Enclosure - Visual Design Details.

The RSU shall comply with *RSU Standard v1.0*, Section 4.3.5.6.2 Tamper Evident Port Design Details.

4.3.4.7.2.7 Operational, Security and other Events Logging - RSU

The RSU shall comply with *RSU Standard v1.0*, Section 4.3.5.13 Logging for General and Security Purposes Design Details.

4.3.4.7.2.8 Operational Logging - TMS

The connected intersection shall fulfill the requirement of 3.3.4.7.2.8 via IOO-specific means, based on principles in the *CIS Controls Implementation Guide for Industrial Control Systems*, Control 6 – Maintenance, Monitoring and Analysis of Audit Logs, and shall provide documentation of how this requirement is met.

4.3.4.7.2.9 Operational Logging - TSC Infrastructure

The connected intersection shall fulfill the requirement of 3.3.4.7.2.9 via IOO-specific means, based on principles in the *CIS Controls Implementation Guide for Industrial Control Systems*, Control 6 – Maintenance, Monitoring and Analysis of Audit Logs, and shall provide documentation of how this requirement is met.

4.3.4.7.2.10 Determine Mode of Operations

The RSU shall comply with *RSU Standard v1.0*, Section 4.2.3 Requirements Traceability Matrix (RTM) Table, FR ID 3.3.3.2.1 Determine Mode of Operations.

4.3.4.7.2.11 Determine Operational Status

The RSU shall comply with *RSU Standard v1.0*, Section 4.3.3.1 Monitor Current Status Design Details.

4.3.4.7.2.12 Determine Operational Performance

The RSU shall comply with *RSU Standard v1.0*, Section 4.2.3 Requirements Traceability Matrix (RTM) Table, FR ID 3.3.3.2.3 Determine Operational Performance.

4.3.4.7.2.13 Determine Operating Environment

The RSU shall comply with *RSU Standard v1.0*, Section 4.2.3 Requirements Traceability Matrix (RTM) Table, FR ID 3.3.3.2.4 Determine Operating Environment.

4.3.4.7.2.14 Access Control Policy

Tasks requiring administrative privileges include the following:

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

If the RSU supports these tasks via its *NTCIP 1218 v01* interface, then it shall be configured such that only an administrator (i.e., an administrative SNMP user) is allowed to perform these tasks in order to comply with this requirement.

If the RSU supports these tasks via its administration interface as specified in *RSU Standard v1.0*, Section 4.3.5.11 Secure Administration Design Details, then the RSU complies with this requirement.

The RSU shall support ongoing privileged access, by requiring periodic (i.e., every 1 hour) re-authentication and hence re-check of administrator privilege.

NOTE: This is to guard against privilege escalation attacks.

These tasks above shall only be carried out if all of the following conditions are met:

- The administrator used a password that meets the requirements for administrative accounts as in the *RSU Standard v1.0*, Section 4.3.5.8.3 RSU Password Design Details.
- The administrator is logged into the RSU directly or via a secure connection using TLS 1.3 or DTLS 1.3 with mutual authentication and client-side certificates.
- The secure session is fresh, i.e., it is torn down after a configurable period of user inactivity (e.g., timeout of 2 minutes). When a login session expires, a re-authentication is required.

4.3.4.7.3 RSU Device Class Design

No design details provided at this time.

4.3.4.7.4 TSC Device Class Design

No design details provided at this time.

4.3.4.7.5 MAP Signer Device Class Design

No design details provided at this time.

4.3.4.7.6 Authenticated Secure Update Design Details

The design details to fulfill the requirements for secure updates of software and firmware follow. These requirements are defined in Section 3.3.4.7.5.

4.3.4.7.6.1 RSU Software and Firmware Updates

The RSU shall comply with *RSU Standard v1.0*, Section 4.2.3 Requirements Traceability Matrix (RTM) Table, FR ID 3.3.1.14 Software and Firmware Updates Requirements.

4.3.4.7.6.2 Trustworthiness of Software and Firmware Updates

The RSU shall implement a vendor-specific mechanism fulfilling all of the following requirements:

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

4.3.4.7.6.3 TSC Infrastructure Software and Firmware Updates

The TSC infrastructure shall implement a vendor-specific mechanism fulfilling all of the following requirements:

- The TSC infrastructure components shall only install software and firmware updates which are either: signed by the TSC component manufacturer; or signed by the IOO (or simply provided by IOO and installed by a user with admin privileges) and then described in documentation. Update packages shall be authenticated by the TSC component before installation.
- Unauthorized rollbacks to previous updates shall be prevented.
- The TSC infrastructure software update system shall protect software update authentication keys from compromise.

If the TSC infrastructure elements are from different manufacturer, then the updates may come from more than one source. It is important for the CI system to ensure that every component only accepts authenticated updates verifiably originated from its own manufacturer [and verified by the CI system to enact changes as intended].

4.3.4.8 Network Monitoring Design

The RSU shall comply with *RSU Standard v1.0*, Section 4.3.5.13 Logging for General and Security Purposes Design Details. This section requires an RSU to log successful and unsuccessful logon attempts.

4.3.4.9 Credential Management Design Details

The design details to fulfill the requirements for credentials management for a connected intersection follow. These requirements are defined in Section 3.3.4.9.

4.3.4.9.1 Credential Provisioning – (D)TLS Design Details

The design details to fulfill the requirements for provisioning a component of a connected intersection with TLS or DTLS client or server certificates follow. These requirements are defined in Section 3.3.4.9.1.

4.3.4.9.1.1 Start-up Initialization

An RSU shall support the secure installation of (D)TLS signing certificates and of the (D)TLS Root (trust anchor) certificate(s) (and any intermediate CA certificates) as per *RSU Standard v1.0*, Section 4.3.5.12.1 Secure Interface for X.509 Credentials for TLS Design Details.

A TSC infrastructure shall support a secure installation of a (D)TLS signing certificate for itself. In addition, a TSC infrastructure shall support secure configuration of the (D)TLS Root Certificate Authority certificate to trust, and optionally its allow-list of TLS end entities that the TSC infrastructure can trust.

A TMS can be initialized by any vendor-specific means.

A Map Data Server need not be initialized for TLS certificate use.

4.3.4.9.1.2 Credential Updates

An RSU shall support the update of (D)TLS certificates and the update of (D)TLS Root certificates (and any intermediate CA certificates) as per *RSU Standard v1.0*, Sections 4.3.5.12.1, 4.3.5.12.2 and 4.3.5.12.3.

A TSC infrastructure should support a secure update of the (D)TLS certificates and the update of (D)TLS Root (trust anchor) certificates (and any intermediate CA certificates) to trust.

The TMS may keep track of the expiration time of RSU certificates and TSC infrastructure certificates and (even) that of the Map Server certificates.

A TMS shall support secure update of its (D)TLS certificates and the (D)TLS Root certificate(s). This update may be vendor-specific.

4.3.4.9.2 Management of Untrustworthy Devices – (D)TLS Design Details

The design details to fulfill the requirements for protecting the system from exchanging data with untrustworthy devices follow. These requirements are defined in Section 3.3.4.9.2.

4.3.4.9.2.1 Monitor Certificate Status

The certificates of the (D)TLS clients that the RSU TLS server connects to shall be monitored for validity, as detailed in Section 4.3.4.6.1.2.2, (D)TLS Authentication - Rejection.

4.3.4.9.2.2 Drop Connections

If an RSU or a TSC infrastructure element, while running or before setting up a TLS or other secure session, finds that the peer device does not have a valid certificate, then the RSU or TSC infrastructure shall immediately close the secure connection or drop the secure connection to that other peer device.

In addition, *RSU Standard v1.0* Section 4.3.5.12.4 Expiration of Credentials Design Details applies.

4.3.4.9.3 Credential System Access – SCMS Design Details

The design details to fulfill the requirements to support SCMS credentials follow. These requirements are defined in Section 3.3.4.9.3.

4.3.4.9.3.1 Connectivity Design

An RSU shall support a secure bootstrapping process at the beginning of its lifecycle, in order to be provisioned with initial SCMS trust material, as per *RSU Standard v1.0*, Section 4.3.5.10.1.1 SCMS Bootstrap Design Details.

An RSU shall support a secure enrollment process for SCMS, as per *RSU Standard v1.0*, Section 4.3.5.10.1.2 SCMS Enrollment Design Details – CAMP or preferably *RSU Standard v1.0*, Section 4.3.5.10.1.3 SCMS Enrollment Design Details – IEEE Std 1609.2.1.

An RSU shall support connecting to an IOO-approved SCMS as per *RSU Standard v1.0*, Section 4.3.5.10.3.1 SCMS Connectivity Design Details – CAMP; or preferably *RSU Standard v1.0*, Section 4.3.5.10.3.2 SCMS Connectivity Design Details – IEEE Std 1609.2.1.

The MAP signer (i.e., the MAP Data Server component in charge of signing MAP messages) shall support a secure bootstrapping process at the beginning of its lifecycle, in order to be provisioned with initial SCMS trust material, similar to the *RSU Standard v1.0*, Section 4.3.5.10.1.1 SCMS Bootstrap Design Details.

The MAP signer shall support a secure enrollment process for SCMS, similar to the *RSU Standard v1.0* Section 4.3.5.10.1.2 SCMS Enrollment Design Details – CAMP or preferably *RSU Standard v1.0*, Section 4.3.5.10.1.3 SCMS Enrollment Design Details – IEEE Std 1609.2.1.

The MAP signer shall support connecting to an IOO-approved SCMS similar to the *RSU Standard v1.0*, Section 4.3.5.10.3.1 SCMS Connectivity Design Details – CAMP or preferably *RSU Standard v1.0*, Section 4.3.5.10.3.2 SCMS Connectivity Design Details – IEEE Std 1609.2.1.

NOTE: How to accommodate an off-site MAP signer is to be determined.

4.3.4.9.3.2 Download SCMS Files

The RSU shall download updated CRLs and SCMS files as in the *RSU Standard v1.0*, Section 4.3.5.10.6.1 Download SCMS Files Design Details – CAMP; or preferably *RSU Standard v1.0*, Section 4.3.5.10.6.2 Download SCMS Files Design – IEEE Std 1609.2.1.

Initially the CAMP design can be supported, but longer term the IEEE Std 1609.2.1 shall be supported.

The RSU knows when to obtain a new CRL from body of the current CRL file it has: the RSU should fetch an updated CRL “within a day of the time indicated by the next CRL field in the current CRL file.”

An arrangement may be supported whereby new CRLs are downloaded by the TMS and then sent to the RSU.

Note: It may be assumed that commonly, new CRLs may be issued approximately every week.

Section 5

Connected Intersection Testing [Informative]

IMPORTANT NOTE TO READERS:

This section of the CI Implementation Guide describes and contains test cases to verify a subset of requirements for SPaT and MAP messages intended for the CI Validation Site Testing to be conducted during the project's period of performance (Spring/Summer 2021).

Other sections of the CI Implementation Guide are intended to address all requirements to create trusted and interoperable connected intersections. Given the project constraints, it is not possible to fully test all the required elements contained in this CI Implementation Guide. To fully validate this CI Implementation Guide, all other elements will need to be tested.

Therefore, this section does not contain a complete set of test cases for a fully conformant connected intersection.

5.1 Introduction to CI Test Cases

5.1.1 CI Testing Scope and Assumptions

Elements Used in the CI Test Cases:

- **RSU.** Device used to broadcast *SAE J2735_202007* SPaT and MAP messages. The test cases do not address any preconditions for RSUs involved during testing. The following assumptions are derived from the basic ability of an RSU to broadcast over-the-air messages:
 - The RSU broadcasts to one or more receivers in range.
 - Communications is one-way, with no feedback to the RSU from any receiver.
 - No error conditions are reported between senders and receivers of messages.
- **SAE J2735 SPaT/MAP Data Receiver.** This element is test hardware and software that is able to act as an OBU/MU to receive over-the-air *SAE J2735_202007* messages, but that has been constructed to provide output data in the JSON format to facilitate determination of Pass/Fail criteria required during testing.
- **IEEE Std 1609.2-2016 Certificates.** SPaT, MAP, and RTCM messages are all signed per *IEEE Std 1609.2-2016* and the relevant security profile:
 - SPaT is signed by the RSU
 - MAP may be signed by the Map Data Server or the TMC
 - RTCM may be signed by the Local Position Correction Generator or the RSU.

The test processes in this document do not address how a signer obtains certificates and do not address where the signing takes place. Additionally, the test processes in this version of this document do not provide a means to check that the signatures on these signed messages are syntactically or semantically correct. Note that messages should only be sent within the system if they are signed, and a message sender should not send a message if they do not have a valid certificate (for example, if they had a valid certificate but it has expired). Therefore, if an RSU is being tested, even though the testing will not validate the *IEEE Std 1609.2-2016* signature, the RSU must EITHER have an up-to-date *IEEE Std 1609.2-2016* certificate OR be running in diagnostic (no-signing) mode as specified in the RSU Standard v1.0.

- **Security Aspects.** The test cases do not address how a signer obtains certificates and do not address where signing takes place.

Note the following regarding RSU outputs:

- The RSU broadcasts such that its transmitted messages may be received by any number of receivers within range
- Communications is one-way, with no feedback to the RSU from the RSU receiver

- No mechanism is defined for the receiver of RSU messages to report error conditions, and so error conditions are not reported or tested

5.1.2 Approach to the CI Test Cases

Role of Test Cases versus Test Procedures:

- This document describes test cases for determining CI verification for SPaT and MAP conformance for the purposes of CI validation sites through the project's period of performance (Spring/Summer 2021), not how to do the conformance.
- Test Cases specify **WHAT** to test. The focus of Test Cases is on data inputs and outputs, and pass/fail criteria. Test Procedures will specify **HOW** to do the Test.
- Test Cases and Test Procedures follow a similar relationship that Requirements and Design have.

Test Cases are Traceable to the In-Scope CI Requirements:

The CI Project is applying a Systems Engineering Process to develop the CI Implementation Guide. One of the objectives of this document is to provide traceability of the proposed test cases to the CI requirements, thus closing the loop between requirements and testing. This traceability is found in Table 14. Requirements to Test Case Traceability Matrix in Section 5.2.

Test Cases are Test Tool and Deployment Agnostic:

- The test cases are written in a test tool agnostic way allowing researchers and deployers, new test tools as well as old, to be considered/used for testing.
- The test cases should be usable across a variety of deployments that may have different design details accounted for in the test procedures and test plans.

5.2 Requirements to Test Case Traceability Matrix (RTCTM)

Table 14 defines the relationships between the requirements found in Section 3.3 of this CI Implementation Guide and the test cases presented in Section 5.3. Only those requirements related to the connected intersection broadcasting a SPaT and MAP payload (data content of the messages) are listed in the table.

To confirm that an implementation fulfills a requirement, the device under test (DUT) shall successfully pass all test cases that trace to that requirement. Several requirements contain the word '(partial)' under the Test Case ID, indicating that additional test cases are needed to fully verify that the requirement is fulfilled.

Table 14. Requirements to Test Case Traceability Matrix

Requirements to Test Case Traceability Matrix (RTCTM)			
FR ID	Functional Requirement	Test Case ID	Test Case
3.3.3	Message Requirements		
3.3.3.1	Message Performance Requirements		
3.3.3.1.1	Uniform Message Requirements		
3.3.3.1.1.1	SPaT Message - SAE J2735	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.1.1.2	SPaT Message - Mandatory Data Elements	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.1.1.3	SPaT Message - CI Mandatory Data Elements	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.1.1.4	SPaT Message PSID	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.1.1.5	MAP Message - SAE J2735	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.1.1.6	MAP Message - Mandatory Data Elements	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.1.1.7	MAP Message - Required Data Elements	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.1.1.8	MAP Message PSID	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.1.3.2	Concise MAP Message Requirements		
3.3.3.1.3.2.1	Nodes by Offsets	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.1.3.2.2	Computed Lanes Requirements		
3.3.3.1.3.2.2.1	Computed Lane - Lane Identifier	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.1.3.2.2.2	Computed Lane - X-Offset	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.1.3.2.2.3	Computed Lane - Y-Offset	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.1.3.2.2.4	Computed Lane - Angle	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.1.5	Timeliness Requirements		
3.3.3.1.5.1	SPaT Message - Broadcast Periodicity	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.1.5.3	MAP Message - Broadcast Periodicity	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.2	Generic Message Requirements		
3.3.3.2.2	Message Revision Requirements		
3.3.3.2.2.1	SPaT Message - Revision Counter Increment	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.2.2.2	SPaT Message - Revision Counter Not Increment	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content

Requirements to Test Case Traceability Matrix (RTCTM)			
FR ID	Functional Requirement	Test Case ID	Test Case
3.3.3.2.2.3	MAP Message - Revision Counter Increment	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.2.2.4	MAP Message - Revision Counter Not Increment	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.2.2.5	MAP Message - Intersection Revision Counter Increment	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.2.2.6	MAP Message - Intersection Revision Counter Not Increment	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.2.3	Timestamp Requirements		
3.3.3.2.3.1	SPaT Message - Message Time Stamp	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.2.3.2	SPaT Message - Intersection Time Stamp	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3	Signal Timing Data Requirements		
3.3.3.3.1	Intersection Identification Requirements		
3.3.3.3.1.1	Intersection Signal Timing Information	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.1.2	Road Regulator Identifier	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.1.3	Intersection Reference Identifier	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.2	Intersection Status Requirements		
3.3.3.3.2.1	Manual Control	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.2.2	Stop Time	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.2.3	Failure Flash	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.2.4	Preemption	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.2.5	Priority	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.2.6	Fixed Time	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.2.7	Traffic Dependent Mode	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.2.8	Standby Mode	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.2.9	Failure Mode	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.2.10	Controller Off	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.2.11	Recent MAP Update	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.2.12	New Lane IDs	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.2.13	No MAP Available	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.2.14	No SPaT Available	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.3	Current Movement State Requirements		

Requirements to Test Case Traceability Matrix (RTCTM)			
FR ID	Functional Requirement	Test Case ID	Test Case
3.3.3.3.3.1	Current Movement State for a Signal Group	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.3.2	Unknown Current Movement State for a Signal Group	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.3.3	Flashing Yellow Arrow Permissive Movement	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.3.4	Protected and Permissive Clearance	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.3.5	Resolve Protected Versus Permissive Movement	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.3.6	Conflict Causes Permissive	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.3.7	No Conflict Causes Protected	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.3.8	WALK State Enumeration (No Conflict)	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.3.9	WALK State Enumeration (Potential Conflict)	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.3.10	Flashing DON'T WALK State Enumeration	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.3.11	Steady DON'T WALK State Enumeration	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.4	Next Movement State Requirements		
3.3.3.3.4.1	Next Movement State	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.4.2	Unknown Next Movement State	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.4.3	No Past State	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.5	Time Change Details Requirements		
3.3.3.3.5.1	Time Change Details	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.5.2	Unknown Time Change Detail	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.5.3	Minimum End Time	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.5.4	Maximum End Time	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.5.5	Unknown Maximum End Time	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.5.6	No Current Movement State Start Time	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.6	Next Allowed Movement Requirements		
3.3.3.3.6.1	Time of Next Allowed Movement	5.3.1.2 (partial)	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.7	Enabled Lanes Indication	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.3.8	SPaT Message - Accuracy	5.3.1.2	SPaT Data Capture 1 – Message Structure and Content
3.3.3.4	Roadway Geometry Data Requirements		
3.3.3.4.1	Intersection Geometry Requirements		

Requirements to Test Case Traceability Matrix (RTCTM)			
FR ID	Functional Requirement	Test Case ID	Test Case
3.3.3.4.1.1	Intersection Geometry Information	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.2	Intersection Geometry - Road Regulator Identifier	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.3	Intersection Geometry - Intersection Identifier	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.4	Intersection Reference Point Requirements		
3.3.3.4.1.4.1	Intersection Reference Point - Position	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.4.2	Intersection Reference Point - Description	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.4.3	Intersection Reference Point Accuracy	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.5	Default Lane Width	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.6	Lane Identifier	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.7	Center of Vehicle Lane Geometry	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.8	Center of Crosswalk Lane Geometry	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.9	Center of Pedestrian Landings Geometry	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.10	Lane Description	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.11	First Node Point - Ingress Vehicle Lane	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.12	First Node Point - Egress Vehicle Lane	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.13	Node Offset from Intersection Reference Point	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.14	Node Elevation Offset from Intersection Reference Point	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.15	Offset from Previous Node	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.16	Elevation Offset from Previous Node	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.17	Advanced Notification - Ingress Vehicle Lane	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.18	End Nodes - Crosswalk Lane	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.19	End Nodes - Pedestrian Landing	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.20	Maximum Distance between Nodes	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.21	Maximum Number of Nodes	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.22	Node Lane Width	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.1.23	Node Accuracy	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.2	Lane Attributes		

Requirements to Test Case Traceability Matrix (RTCTM)			
FR ID	Functional Requirement	Test Case ID	Test Case
3.3.3.4.2.1	Direction of Travel	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.2.2	Lane Sharing	5.3.2.2 (partial)	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.2.3	Lane Type Attributes	5.3.2.2 (partial)	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.2.4	Lane Attributes - Vehicle	5.3.2.2 (partial)	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.2.5	Lane Attributes - Crosswalk	5.3.2.2 (partial)	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.2.6	Lane Attributes - Bicycle	5.3.2.2 (partial)	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.2.7	Lane Attributes - Tracked Vehicles	5.3.2.2 (partial)	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.2.8	Lane Attributes - Parking	5.3.2.2 (partial)	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.3	Lane Maneuvers	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.4	Connections Between Lanes		
3.3.3.4.4.1	Lane Connections	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.4.2	Connection Egress Lane	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.4.3	Connection Maneuvers	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.4.4	Connection Signal Group	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.5	Speed Limit Information Requirements		
3.3.3.4.5.1	Default Speed Limit	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.5.2	Change in Lane Speed Limit	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.6	Revocable Lanes	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.7	MAP Message - Accuracy	5.3.2.2	MAP Data Capture 1 – Message Structure and Content
3.3.3.4.8	Signal Timing and Roadway Geometry Information Synchronization		
3.3.3.4.8.1	Matching Intersection Reference Identifier	5.3.3.1	SPaT-MAP Data Consistency

5.3 CI SPaT Test Cases

5.3.1 CI SPaT Test Case

5.3.1.1 CI SPaT Test Case Overview

Figure 36 is an illustration identifying the relevant data flows used in the CI SPaT Data Stream Capture Test Cases.

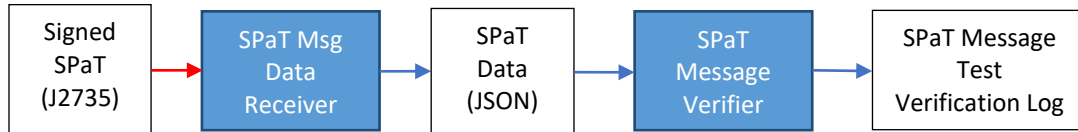


Figure 36. CI SPaT Message Data Structure and Content Test Case Diagram.

Testing Notes

The Signal Timing Information sent to RSU will be verified as an output of the RSU, as captured by the SPaT Msg Data Receiver. The input Signal Timing Information sent to the RSU will not be tested. Whether the RSU has valid certificates will not be tested.

5.3.1.2 SPaT Data Capture 1 – Message Structure and Content

Test Case	
ID: TC-SPaT Data-Capture-1	Title : SPaT Data Capture – Message Structure and Content
Purpose:	TC Purpose: Verify format, message content values, and structure of SPaT data stream output from RSU are correct per <i>SAE J2735_202007</i> and the CI Implementation Guide.
Objective:	The objective of this test case is to verify system interface between an RSU and RSU Message Receiver. The test case verifies that the SPaT message broadcast from the RSU contains all the mandatory OBJECTS, and that the OBJECTS conform with the valid value ranges as specified in <i>SAE J2735_202007</i> and the CI Implementation Guide.
Inputs:	<u>Input Data Specifications</u> <ul style="list-style-type: none"> Table 7 contains a complete SPaT data specification.
Expected Outcome(s):	All SPaT data and message structure are verified as correct, including: structure of data and valid value of data content.
Feature Pass/Fail Criteria:	<u>Data Verification Outcomes:</u> <ul style="list-style-type: none"> Pass: <ul style="list-style-type: none"> All mandatory SPaT data elements (OBJECTS) within the message are verified as correct. Message structure of SPaT is correct. Fail: Any other outcome.
Preconditions:	<ul style="list-style-type: none"> Either the RSU has <i>IEEE Std 1609.2-2016</i> certificates and can sign (preferred), or the RSU is in diagnostic mode per the <i>RSU Standard v1.0</i> and is creating non-secured data in the format specified in that standard. Every device (RSU) is certified prior to testing against the CI testing defined herein.

5.3.2 CI MAP Test Cases

5.3.2.1 CI MAP Data Capture Stream Tests

Figure 37 is an illustration identifying the relevant data flows used in the CI MAP Message Level Test Cases.

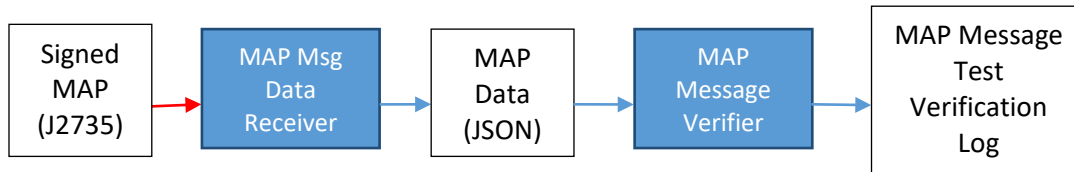


Figure 37. CI MAP Message Data Structure and Content Test Case Diagram.

Testing Notes.

The Intersection Geometry Information sent to RSU will be verified as an output of the RSU, as captured by the MAP Msg Data Receiver. The input Intersection Geometry Information sent to the RSU will not be tested. Whether the RSU has valid certificates will not be tested.

5.3.2.2 MAP Data Capture 1 – Message Structure and Content

Test Case	
ID: TC-MAP-Data-Capture-1	Title: MAP Data Capture – Message Structure and Content
Purpose:	TC Purpose: Verify format, message content values, and structure of MAP data stream output from RSU are correct per <i>SAE J2735_202007</i> and the CI Implementation Guide.
Objective:	Objectives to verify: <ul style="list-style-type: none"> Every MAP message an RSU broadcasts is a valid MAP message.
Inputs:	<u>Input Data Specifications</u> <ul style="list-style-type: none"> Table 9 contains a complete MAP Data specification.
Expected Outcome(s):	All MAP data and message structure are verified as correct, including: structure of data, and valid value of data content.
Feature Pass/Fail Criteria:	<u>Data Verification Outcomes:</u> <ul style="list-style-type: none"> Pass: <ul style="list-style-type: none"> All mandatory MAP data elements (OBJECTS) within the message are verified as correct. Message structure of MAP is correct. Fail: Any other outcome.
Preconditions:	<ul style="list-style-type: none"> The MAP is validly signed, either by the RSU or by a center node as discussed above. Every device (RSU) is certified prior to testing against the CI testing defined herein.

5.3.3 CI SPaT-MAP Data Consistency Test Case

The figure below is an illustration identifying the relevant data flows used in the CI SPaT-MAP Data Consistency Message Level Test Cases.

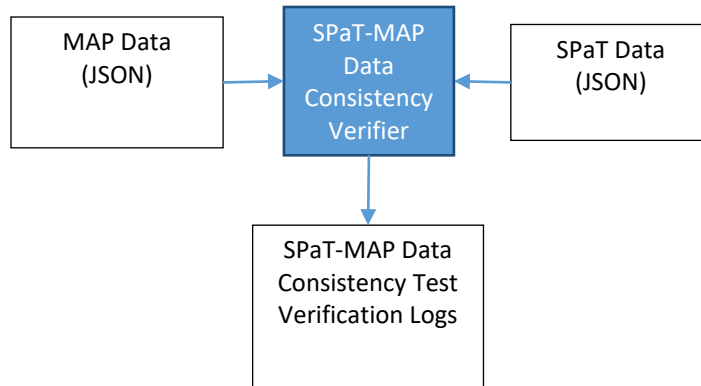


Figure 38. CI SPaT-MAP Data Consistency Test Case Diagram.

5.3.3.1 SPaT-MAP Data Consistency

Test Case	
ID:TC-SPaT-MAP-Data-Consistency-1	Title: SPaT-MAP Data Consistency
Purpose:	Verify data consistency between SPaT and MAP for the following data elements from <i>SAE J2735_202007</i> : <ul style="list-style-type: none"> • DE_RoadRegulatorID • DE_IntersectionID
Objective:	<u>Objectives to verify:</u> <ul style="list-style-type: none"> • RSU broadcasts valid SPaT and MAP messages that are consistent.
Inputs:	<u>Input Data Specifications</u> <ul style="list-style-type: none"> • Table 7 contains a complete SPaT Data specification. • Table 9 contains a complete MAP Data specification.
Expected Outcome(s):	Data consistency between MAP and SPaT data are verified as correct for the specific data elements defined in the Purpose section of this test case.
Feature Pass/Fail Criteria:	<u>Data Verification Outcomes:</u> <ul style="list-style-type: none"> • Pass: <ul style="list-style-type: none"> - Referential integrity between MAP and SPaT is verified for the specific data elements defined in the Purpose section of this test case. • Fail: Any other outcome.
Preconditions:	<u>Dependencies:</u> Must have executed and passed: <ul style="list-style-type: none"> • Test Case 3.2.1 SPaT Data Capture 1 – Message Structure and Content • Test Case 3.3.1 MAP Data Capture 1 – Message Structure and Content

Annex A

Connected Intersection Traffic Controller Issues & Recommendations [Informative]

This annex is a draft that is intended to be updated based on design information that is being added to Section 4.3.2, TSC Infrastructure to RSU Design Details.

A.1 Issues & Rationale

A Connected Intersection (CI) is defined as an infrastructure system that broadcasts Signal, Phase, and Timing (SPaT), mapping information, and positional correction data to directly vehicles via a Roadside Unit (RSU). A collaborative effort has formed to address a number of ambiguities and gaps identified by early deployments and provides guidance for providing messages and developing applications for signalized intersections that are truly interoperable across the United States, especially for automated transportation systems. The CI Committee has focused early efforts on addressing gaps and lessons learned from early CV deployments, with special focus on Red Light Violation Warning (RLVW) applications within passenger vehicles.

This Annex summarizes the Traffic Controller Issues Task Force (TCI TF) discussions, including the controller vendor subgroup discussions per our objective to establish a consistent set of assumptions and criteria when generating SPaT data from within NTCIP 1202-based traffic controller firmware. This commonality aims to reduce the vendor-specific ambiguity of controller generated SPaT data as well as seeks to improve the determinism and quality of SPaT data when sourced by *NTCIP 1202 v03A* based traffic controllers.

This Annex is offered to be distributed within the various CI Task Forces for broader input and continued revision. The TCI TF has discussed these assertions across several weeks' meetings with expected output as suggested recommendations to the ITE, NTCIP, SAE and other working groups that many of us also participate within. It is expected that these standard working groups will take these recommendations and make the appropriate updates to their recommended practices, and/or respective standards.

A.1.1 NTCIP 1202 v03A Traffic Controller SPaT Data Ambiguity

SPaT challenge deployments have revealed several areas of ambiguity when SPaT message payloads are generated from traffic controllers.

A.1.1.1 Vendor Ambiguity

Various traffic control vendors have interpreted the data elements differently, leading to vendor discrepancy within SPaT message data fields for a given intersection configuration. One commonly discussed example is the definition of the MinEndTime under signalized green rest. It is a goal for the connected intersection to provide a consistent SPaT data value for a given intersection configuration and operational state, regardless of controller vendor.

A.1.1.2 SPaT Generation under Special Situations

There has been an inconsistency of the operational conditions when SPaT is actively generated, versus those conditions when SPaT generation is inhibited. It is a goal for the connected intersection to provide SPaT data during all possible times and conditions of signalized operation including non-standard scenarios. This includes, but is not limited to, startup, flashing, manual control, and preemptive operation.

A.1.2 Conflict between Gap-Based traffic control practices and the predictive signalization needs for RLVW applications

Red light violation warning (RLVW) has been identified by the CI Committee as a vehicle safety application that should be supported by connected intersections in the near term. Early SPaT deployments have revealed a disconnect between the in-vehicle application's need for a deterministic end of green warning, versus the inherently indeterministic nature of gap-based traffic control. The TCI TF does not want to adversely affect the well-established infrastructural safety system of gap-based green termination. At the same time, it is recognized that a deterministic end of green interval can provide safety benefit to CVs. The TCI TF has developed a method to set deterministic end of signal indications called Assured Green End Time (AGET), Assured Yellow End Time (AYET) and Assured Red End Time (ARET).

A.1.3 Determinism and Consistency for TimeChangeDetails within the SPaT Message

The SPaT message offers TimeChangeDetails that will allow in-vehicle and other external systems to access the traffic controller's estimates for the future state timing of the traffic signals. Prior work within the Connected/Automated Vehicle standards do not provide sufficient detail on the use cases, nor requirements of the connected intersection when populating these time marks. The TCI TF is offering a recommended implementation of these time marks as an effort to improve the consistency and usefulness of this predictive data. These recommendations are not grounded in a use-case-driven, systems engineering process, but rather offers a consistently implementable improvement to the expected values that *NTCIP 1202 v03A* traffic controllers can generate.

The TCI TF has delved into the details of SPaT generation and offered a more detailed methodology for the traffic controller's computation of SPaT data to resolve these three problem statements. This document provides an overview of these methods. At the end, a consolidated set of recommendations is detailed with targeted intent for the various SDOs, IOOs, vendors, and other practitioners in support of these methods.

A.2 Proposed Resolution to NTCIP 1202 Traffic Controller SPaT Data Ambiguity

In an effort to reduce ambiguity and vendor-specific implementation of SPaT, the TCI TF established a subgroup of controller vendors to discuss their respective assumptions and implementation of SPaT. It was determined that an underlying set of base assumptions and established level of detail should be adhered to by all vendors when implementing SPaT. This will ensure that SPaT generated with consistency given the *NTCIP 1202 v03A* configuration of the traffic controller as well as generated for all operational modes of traffic control. This following section provides the base assumptions and input parameters that all *NTCIP 1202 v03A* traffic controllers should apply when generating SPaT.

A.2.1 Base Assumptions when Generating SPaT

A.2.1.1 Active TOD Control

SPaT shall be generated by the traffic control firmware under assumption that the currently active time of day plans (Event Plan), input driven commands, or active pages will remain currently active. This is to include coordination patterns, timing plans, sequence tables, and other "pages" that are run on a time-of-day basis and/or triggered from a variety of potential sources. Traffic controller's SPaT data can be enhanced to "look ahead" into pending plans, patterns, sequences, and pages that are soon to become active, but this will not be a requirement of the control firmware.

A.2.1.2 Active Preemption Control

SPaT shall be generated under assumption that any inactive preemption, NTCIP 1211, or SRM requests will remain inactive and any active priority requests will remain active until served. The controller firmware shall update SPaT values within one second upon receiving changes to priority control inputs.

A.2.1.3 Active Demand

SPaT shall be generated under assumption of any active demand for phase or pedestrian service. This demand can be sourced from cabinet inputs, central system commands, controller configuration, internal logic, or various other means. SPaT shall generate its values upon current demand (Phase/Ped calls) and be updated within one second upon changes to this demand. Please note that the demand need not be actively serviceable to be considered in the SPaT message. As example, a coordinator may omit a phase until its permissive window opens, however SPaT shall consider this phase to have serviceable demand with expectation of future opening of this permissive window.

A.2.1.4 NTCIP 1202 v03A Configuration

SPaT shall be generated with consideration of the NTCIP configuration of the traffic controller for those objects listed below in Annex A.5, NTCIP 1202 Objects: SPaT Generation Conformance. These objects form the minimal basis of consideration for SPaT generation. Vendors are encouraged to improve the accuracy of SPaT by incorporation of additional features or algorithmic logic, however, this minimal set of features within Annex A.5, if supported by the traffic controller, shall be factored into SPaT generation. There is not a documented basis for “factoring” in these features. It is expected that each traffic controller vendor maintains active timers for these features and can compute the expected phase sequence and timing intervals using these internal mechanisms. SPaT shall be updated within one second after any consistency checks and transactional database changes are applied to the traffic controller.

Example: If the traffic controller supports options to include *MUTCD* 3 second all red pedestrian clearance, pedestrian change through yellow, and pedestrian change through red, then the TimeMark generated for the end of green estimation must be adjusted based upon the pedestrian timing to include these 3 features if enabled as follows:

TimeMark >= Current Time
+ Pedestrian Walk Time Remaining
+ Pedestrian Change Time Remaining
+ *MUTCD* 3 Second Pedestrian Clearance (if enabled)
– Pedestrian Change Through Yellow (if enabled)
– Pedestrian Change Through Red (if enabled)

A.2.1.5 Soft Flashing Operation

SPaT shall be generated when the traffic controller is in soft flash operation (flash through phase loadswitch). Any special sequencing that is applied to enter and exit soft flash shall be supported when activated. The traffic controller shall try to estimate any known timing intervals that condition the flash entry or exit intervals and sequences (e.g., preemption flash min dwell).

A.2.1.6 Hard Flashing Operation

NTCIP 1202 v03A traffic controllers do not currently have awareness of the signal indication state during hard flash (Flash through flash transfer relays) unless offered via proprietary configurations. SPaT signalization and timing data cannot not be required to be generated when the traffic controller is in hard flash operation due to this lack of awareness. There is, however, a considerable limitation if hard flashing operation cannot be communicated via SPaT messaging. The CI Committee will make recommendations to the *NTCIP 1202 v03A* working group to update *NTCIP 1202 v03A* to include configuration of signal output status when in hard flash operation. Upon this update to *NTCIP 1202 v03A*, the traffic controller shall broadcast signal head status when under hard flash operation.

There is additional risk DC isolator failure may remove controller awareness of flashing conditions. The CI Committee recommends NEMA and ATCC cabinet standards consider addition of MMU/CMU interlock inputs (similar to RR preemption interlock circuitry) to ensure controller awareness of flashing operation. The duration of hard flashing operation is usually unknown. However, the current duration of flash provides some insight as to how much longer the flash conditions may persist.

A.2.1.7 Tech Flash

When the controller is placed in Tech Flash (Hard flash without stop time), the traffic controller shall offer SPaT consistent to Hard Flashing operation and not generate SPaT consistent to the internal timing of the controller, which may be cycling at this time. It is assumed that it is more important for SPaT to match the roadway signalization rather than internal controller logic. Some cabinet variations do not have flash sense inputs. The CI Committee recommends agencies to ensure flash sense inputs are mapped into the traffic controller whenever SPaT is generated.

A.2.1.8 Stop Time

When the controller receives a stop time input, the active (frozen) controller state on the affected (stopped) ring shall remain as the basis for SPaT generation. Since stop time duration is unknown, the confidence factor will be adjusted, however the SPaT output will remain consistent to the current phase timers. If this form of stop time input allows continuation of countdown timers for clearance intervals or other timers, SPaT shall be adjusted accordingly.

A.2.1.9 Manual Control

When the controller receives an MCE or Manual Advance input, the SPaT generation shall be updated accordingly to be consistent with the current set of possible dwell/advance options. The TimeChangeDetails shall be adjusted accordingly.

A.2.1.10 Output Mapping

SAE J2735_202007 describes signal state data elements and MAP data so that external roadway users can understand the current and future state signalization of the roadway. This status is provided in a simplified format using MovementPhaseState and TimeChangeDetails to represent the roadway indications. This mapping implies an assumption that the traffic controller can map its perceived signal timing into the to the signal indications (Signal Groups) that are presented to the roadway users. In real-world applications, this is not always the case. Overlaps, Controller I/O processing, In-Cabinet output panels, and other possible esoteric applications can have impact to override the actual signal outputs that are displayed to the roadway users to control their movements on associated Lane IDs. Given the critical nature of SPaT messages for real-time safety applications, intersections that generate SPaT data must remove any in-cabinet output panels, controller output logic processing, or other post-processed means of output override that would render the SPaT data inaccurate relative to the signal group displays above the roadway. In cases where overlaps are mapped to control the signal outputs, it is the responsibility of the traffic controller to generate SPaT consistent to the overlap and/or phase states that are actively controlling the signal group. This output assignment often occurs on a time of day and/or preemptive basis and cannot easily be performed outside the traffic controller itself. If the traffic controller is both independently controlling phase timing as well as generating the SPaT message, it must consider all internally known details that will affect the controller-level outputs prior to establishing these TimeChangeDetails.

The CI Committee makes the recommendation to the *NTCIP 1202 v03A* working group to establish lookup tables that allow the traffic controller firmware to have an accurate mapping of phase and overlap outputs relative to the roadway signalization on a LaneID and allowable maneuver basis. This lookup table shall also contain information regarding generic I/O states that may illuminate blank out signs that affect allowable maneuvers relative to signal timing. Some of the requirements of this table shall include discernment of the following:

- TOD Event Plan or other basis for dynamic changes to I/O mapping
- Various forms of roadway signal heads including FYA, right turn arrows, five section left turn heads, blank out signs, physical signage for TOD based allowable maneuvers, reversible/restricted lanes by TOD basis
- Advanced phase and overlap modes

A.2.1.11 Proprietary Features

Vendors are encouraged, but not required to implement SPaT for proprietary controller features. Those features that impact the features listed in Annex A.5, NTCIP 1202 Objects: SPaT Generation Conformance, shall be assumed to be incorporated into SPaT when these dependent features are affected (e.g., Minimum Green affected by proprietary queue measurement techniques).

A.2.1.12 Externally Coordinated and/or Adaptively Controlled Intersections

In these cases, the resultant signal state durations are not being decided by the traffic controller but rather an external process that is asserting a higher-level control over the traffic controller. The traffic controller may be commanded to run free, hold-on-line, or run specific coordination patterns by the external control process that are then manipulated in real time by hold/force-off/omit or other remote commands. SPaT messages generated by the traffic controller in these cases will not be accurate to the future state control commands that are offered by the external process. As example, an intersection running under an external command to free or hold on-line, may not have awareness of serviceable side street demand or pending force off commands, that are being managed by the external process. In these cases, the external process must carry the responsibility to distribute the SPaT messages since it alone knows the likely future state of the intersection. It, however, may not have awareness of cabinet I/O, preemptive control, or other higher priority actions within the traffic controller. One recommended approach here is for the traffic controller to issue a unicast SPaT message to only this external process, which then can override SPaT TimeChangeDetails and transmit the final SPaT message to the RSU, providing accuracy to both the awareness of the local controller as well as overridden values for those situations where the external process has better future-state awareness.

A.2.1.13 Post-processed SPaT generation

There are expected cases where the SPaT message is not generated by the traffic controller, but rather a separate device that is observing the operation of the traffic controller. This could include MMU/CMUs that are observing the actual field outputs, or a process that is performing NTCIP polling of the traffic controller status and issuing SPaT messages on behalf of the traffic controller. These methods will be limited in their knowledge of the inner-workings of the traffic controller, however, offer some means to retro-fit SPaT functionality to intersections running legacy control equipment which cannot support SPaT message generation.

In these cases, the device that is generating the SPaT message is not likely to be able to handle more detailed cases, such as timed overlaps, preemptions, and/or flash events. Given the critical safety nature of SPaT messages, it is recommended that this approach be taken only when the signals are running simple sequences and conditions that the post-processed SPaT generator can accurately represent.

A.2.2 Special Traffic Control Situations

There are several common traffic control situations that were not explicitly detailed in earlier versions of *SAE J2735_202007*. This has led to either a discontinuance of SPaT messaging during these conditions, and/or varied vendor interpretation of the Time Change Details. The following guidance is offered for these special situations to resolve any ambiguity and ensure SPaT messaging can be supported in these situations.

A.2.2.1 Changes between Permissive and Protected Movements without a Clearance Interval

There is a common case here when a flashing yellow arrow (permissive left) will revert directly to a protected left green arrow. These time change details may lead roadway users to assume these time marks are the time when change will occur from a protected or permissive movement into a restricted movement and not realize this change can occur between protected and permissive movements. The TimeChange detail shall indicate the following:

nextTime = likelyTime for cases when the movement will shift between protected and permissive movements, without a clearance interval present.

nextTime = likelyTime + Clearance Interval for cases when the movement will shift between protected and permissive movements, with an interim clearance interval present.

A.2.2.2 Movement into or Revert from Flashing Operation

Many signals will have an operation where the main street movement flashes yellow (common in late night operation). This can be handled via the flash transfer relays in the cabinet where the traffic controller is sitting in a dormant state or can be configured to be output by the traffic controller through the normal load-switches. When the signal goes from flashing yellow into normal operation, it is allowable for it to go through a yellow clearance or revert directly into green. These cases present some real safety concerns as drivers under a flashing red will enter the intersection upon assumption that this state will not change immediately.

To safely allow SPaT-guided vehicle movements through this scenario, it is recommended that the traffic controller be configured to drive flashing outputs through the phase load-switches and not flash transfer relays. It is additionally recommended that reversion from flashing operation go through a full yellow and/or all red clearance interval, and not directly revert into green operation. This restricted operation will ensure the traffic controller can assert SPaT message guidance during flashing operation, as well as through the return to normal phase sequencing.

A.2.2.3 Bike/Transit Movements

Agencies have deployed signalized control for bike and transit modes of travel via vendor-specific features and creative signal sequencing. There are cases where separate lanes and/or signalization can be given to specific modalities. There are often roadway signals specific for transit vehicles and bicycles that do not follow the *MUTCD* guidance of green balls or arrows. One example is a white bar that is displayed for transit (LRT/Bus) operators to proceed into the intersection while all other indications are held red (Queue Jumping). As another example, there are various new pedestrian and bicycle displays that allow these users early entry into the intersection prior to the green indications being provided for vehicles sharing the same movement. For SPaT messaging to handle these cases, it is recommended that a separate SignalGroupID be generated for any mode designation that may be independently controlled from the other lanes on the roadway. As example, a bike or transit-only lane should be given its own SignalGroupID that is representative of the roadway indications given to the cyclists and/or transit vehicles. This type of configuration will allow the traffic controller to generate accurate SPaT information for these SignalGroupIDs in these cases and not leave an oversimplification that these lanes have the same attributes as for the associated vehicle movements.

A.2.2.4 Green Select Operation

A common situation that has been difficult to characterize with SPaT is the case of a phase resting in green awaiting service on conflicting movements. The time mark for this case can either reflect a minimum time to change of 0.1 second or 0.0 seconds, a likely time that is very indeterminate, and a maximum time that can be for even hours in late night operation. It is recommended that 0.1 second be used as the minimum time to change, rather than 0.0. 0.0 should be reserved for the case where green termination was commanded, and the field outputs change is imminent. A vehicle resting in green may display 0.1 second for an indefinite period with increased value to match the active passage timer if/when additional vehicle actuations on the movement reset the passage timer.

A.3 Proposed Resolution to Determinism and Consistency for TimeChangeDetails within the SPaT Message

The TCI TF has discussed means to improve the time change details to remove ambiguity beyond the improvements provided in the prior problem statements. This section details assumptions and deployment guidance for the traffic controller's generation for each of the TimeChangeDetails elements.

A.3.1 **startTime TimeMark OPTIONAL**

This time mark defines the point in time when a future interval is estimated to begin. In order to avoid ambiguity in the meaning of the time mark, the time mark is always considered to be a time in the future. Therefore, time mark cannot be used for intervals that have already begun timing.

The TCI TF recommends that this time mark be made mandatory and not optional for future states but not be present for current states.

A.3.2 **minEndTime TimeMark**

This time mark defines the shortest point in time when the signal group may terminate is current indication as output by the traffic controller assuming current demand and operational conditions (preemption state, etc.). This time mark must take into consideration all active phase calls, preemption requests, or other demand inputs at the time of SPaT message generation, but does not need to provide the absolute minimum end time for demand inputs that have not yet been received. The end time shall be generated in accordance with the following rules:

For Green Indications of movements that are currently running in actuated mode:

TimeMark = Current Time
+ Minimum Green Timer Remaining for controlling phase (if any)
+ Gap (Passage) Timer Remaining if less than Minimum Green Timer
+ Trailing Overlap Green Timer if signal group is currently being controller by an overlap that will time its trailing green based upon current demand.

For Green Indications of movements that are currently in a non-actuated mode:

TimeMark = Current Time
+ Maximum Green or Split Max Timer Remaining for controlling phase (if any)
+ Trailing Overlap Green Timer if signal group is currently being controller by an overlap that will time its trailing green based upon current demand.

For Green Indications of movements that are actively timing a pedestrian phase that must terminate with the controlling movement, the Time Mark established above must be adjusted based upon the pedestrian state.

TimeMark >= Current Time
+ Pedestrian Walk Time Remaining
+ Pedestrian Clearance Time Remaining
+ MUTCD 3 Second Ped Clearance (if applicable)
– Ped Clearance Through Yellow (if applicable)
– Ped Clearance Through Red (if applicable)

For Yellow Indications of movements:

TimeMark = Current Time
+ Yellow Timer for phase or overlap that is currently controlling the signal group.

For Red Indications of movements:

TimeMark = Current Time
+ Expected minimum duration of all movements that have active demand prior to service of the phase or overlap will next control this signal group.

In cases of an active Preemption, the aforementioned intervals may be programmed to run override values. The generation methods above shall remain valid; however, the traffic controller must substitute

the preemptively overridden timing values upon controller activation of the preemptive timing (may occur before or after preemption input delay interval).

The TCI TF recommends that this time mark be made mandatory and not optional.

A.3.3 maxEndTime TimeMark OPTIONAL

This time mark defines the longest point in time when the signal group may terminate is current indication as output by the traffic controller. This time mark must take into consideration all active phase calls, preemption requests, or other demand inputs at the time of SPaT message generation, but does not need to provide the absolute minimum end time for demand inputs that have not yet been received or consider the possibility of the removal of an actively received demand inputs. The end time shall be generated in accordance with the following rules.

For Green Indications of movements that are currently running in actuated mode:

TimeMark = Current Time
+ Maximum Green or Maximum Split Timer remaining for controlling phase (whichever is greater, if either apply)
+ Added Extension Timer Remaining (if this feature is enabled and current demand will require added extension)
+ Trailing Overlap Green Timer if signal group is currently being controller by an overlap that will time its trailing green based upon current demand.

Note: Maximum Split Timer is defined as the time to phase force off if running under a coordinated or preempted mode.

Note: In cases where no conflicting demand is present, this Time Mark will be set to the value for unknown.

For Green Indications of movements that are currently in a non-actuated mode:

TimeMark = Current Time
+ Maximum Green or Split Max Timer Remaining for controlling phase (if any)
+ Trailing Overlap Green Timer if signal group is currently being controller by an overlap that will time its trailing green based upon current demand.

For Green Indications of movements that are actively timing a pedestrian phase that must terminate with the controlling movement, the Time Mark established above must be adjusted based upon the pedestrian state.

TimeMark >= Current Time
+ Pedestrian Walk Time Remaining
+ Pedestrian Clearance Time Remaining
+ MUTCD 3 Second Ped Clearance (if applicable)
– Ped Clearance Through Yellow (if applicable)
– Ped Clearance Through Red (if applicable)

For Yellow Indications of movements:

TimeMark = Current Time
+ Yellow Timer for phase or overlap that is currently controlling the signal group.

For Red Indications of movements:

TimeMark = Current Time

+ Expected maximum duration of all movements that have active demand prior to service of the phase or overlap will next control this signal group.

The TCI TF recommends that this time mark be made mandatory and not optional.

A.3.4 likelyTime TimeMark OPTIONAL, (along with TimeIntervalConfidence)

This time mark has already been applied in practice along with the associated TimeIntervalConfidence for green indications. The confidence factor requires a cycle-by-cycle and/or historic statistical analysis of signal timing that is beyond the capabilities of *NTCIP 1202 v03A* standard traffic controllers. Rather than undermine the existent deployments of this data field, the TCI TF has decided to leave this field as optional and suggest this field be populated by external systems that are performing this statistical analysis.

This time mark is not currently being used for red signal indications and is again suggested to be left alone by the traffic controller and utilized by external systems that are performing a statistical analysis of signal timing.

The predictive nature of signal timing is expected to be characterized and bounded using the minEndTime and maxEndTime for all indications (R,Y,G). A mean value for green duration is not available unless the traffic controller has capability to generate this likely time and interval confidence. In cases where the green duration is deterministic (fixed time, max recall, etc.), the minEndTime will equal the maxEndTime revealing this level of certainty to the end user.

The TCI TF recommends that this time mark remain optional.

A.3.5 nextTime TimeMark OPTIONAL

This element is likely to be used to determine the wait state for the next occurrence of service of an active green movement, not to be set as zero if the current movement is green. This is a best predicted value based upon awareness of the intersection. Full demand of all phases can be assumed unless the traffic controller is capable of monitoring current phase usage and can more accurately estimate future split/phase utilization. This value should include the time to service full demand for all phases that precede the next beginning of green service of the current signal group.

In coordinated operation, this value shall establish the time mark for the next service of the phase based upon the continued in-step coordinated operation and timing commensurate to the regular permissive/split window of the phase. In cases of coordinated transition or transit signal priority, accuracy can be improved if the split adjustment methodologies are factored into this value computation. This improvement is desirable, but not mandatory for the traffic control to apply.

In free operation, this value shall establish the time mark for the next service of the phase based upon current intersection demand. If the traffic controller can apply data for recent average green timing of each phase (split monitor), it will improve this estimate. However, at a minimum, the traffic controller shall generate this value assuming minimum green timing of all active calls to preceding phases as well as assuming pedestrian service for all actively registered pedestrian demand.

The TCI TF recommends that this time mark be made mandatory and not optional.

A.4 Recommendations

A.4.1 Assumptions of elements to be handled externally from this TF

BSM authentication will be managed externally to the traffic controller and any receipt of BSM by the traffic controller can be treated as authenticated.

A.4.2 Traffic Controller Vendors

- Controller firmware shall be modified to support SPaT generation consistent with these NTCIP object recommendations.
- Controller firmware shall be modified to support SPaT generation consistent with this AWEG operation. – which includes the following:
 - Controller firmware must be updated to receive and have awareness of GID
 - Controller firmware must be updated to received BSM messages.
 - Controller firmware must be updated to locate current detection inputs upon the GID.
- Controller firmware shall be modified to support Next Time which includes the following:
 - Awareness of future cycle coordinated split timing
 - Awareness of free-run effective cycle timing.
- Upon update to *NTCIP 1202 v03A* for hard flash roadway colors, the traffic controller shall broadcast signal head status when under hard flash operation.
- The traffic controller shall support unicast SPaT message payload to external processes, which then can override SPaT TimeChangeDetails and transmit the final SPaT message to the RSU.

A.4.3 NEMA TS-2/ATCC

- There is risk DC isolator failure may remove controller awareness of flashing conditions. The WG recommends NEMA and ATCC cabinet standards consider addition of MMU/CMU interlock inputs (similar to RR preemption interlock circuitry) to ensure controller awareness of flashing operation.

A.4.4 NTCIP 1202 WG

- New traffic controller configuration elements (MIB objects) should be defined for the placement of detection zones relative to the GID as well as decision support options for dynamic AWEG decisions.
- The CI committee will make recommendation to the *NTCIP 1202 v03A* working group to update *NTCIP 1202 v03A* to include configuration of signal output status when in hard flash operation.

A.4.5 SAE J2735 WG

- Guidance provided to disuse likelyTime for RLWV applications and instead suggested use of minEndTime = maxEndTime when the AWEG decision is rendered. Description that this decision will be rendered with at least 2.0 seconds of advance warning time by a Connected Intersection.
- Guidance provided to use NextTime for ECO drive and other applications. minEndTime and MaxEndTime will provide boundaries to NextTime estimate when signal indication is red.
- GID shall include standard provision to locate detection zones (stop line and advance).
- TimeChangeDetails are recommended to all be mandatory, except likelyTime and confidence factor, which are recommended to not be populated by an *NTCIP 1202 v03A* signal controller.

A.4.6 ITE

- Signal Timing Manual: Clearance intervals are defined relative to safe passage of vehicles to the end of the intersection “box,” not the end of opposing crosswalk, this should be addressed in the red clearance interval recommendations within the STM.
- Signal Timing Manual: STM is recommended to include description and examples of AWEG operation.
- Detection Handbook: The handbook should be updated to provide examples of detailed detector configurations for AWEG.

A.4.7 IOOs

- ATC traffic control firmware is recommended to be updated to firmware that supports these recommendations.
- Detection zones shall be extended where feasible to accommodate AWEG.

- Signal timing strategies that use dynamic red/yellow clearance intervals shall be converted to static clearance intervals.
- MAPs (GID) shall be generated to include approach beyond dilemma zone.
- MAPs (GID) shall be generated to include detector placement.
- The TF recommends agencies to ensure flash sense inputs are mapped into the traffic controller whenever SPaT is generated.
- It is recommended that external system SPaT generation only be applied when the signals are running simple sequences and under conditions that the post-processed SPaT generator can accurately represent.
- it is recommended that the traffic controller be configured to drive flashing outputs through the phase load-switches and not flash transfer relays.
- It is additionally recommended that reversion from flashing operation go through a full yellow and/or all red clearance interval, and not directly revert into green operation.
- When designated pedestrian and bicycle signalization is provided to roadway users that allow these users early entry into the intersection prior to the green indications being provided for vehicles sharing the same movement, it is recommended that a separate SignalGroupID be generated for any mode designation that may be independently controlled from the other lanes on the roadway.

A.5 NTCIP 1202 Objects: SPaT Generation Conformance

The following listing of *NTCIP 1202 v03A* objects is a listing of those that are required to be factored into the generation of SPaT when sourced from an *NTCIP 1202 v03A* traffic controller. The CI Committee will make recommendations to the NTCIP 1202 WG that a new attribute be included in the object definition or description as to the impact of these objects upon SPaT. Some of these objects and how they affect SPaT should fully self-explanatory, (e.g., dual entry is highlighted below so that type of call should be treated as demand when applicable). Others may require more detailed guidance for how the object is to be applied.

```
PhaseEntry ::= SEQUENCE {
phaseNumber          INTEGER,
phaseWalk            INTEGER,
phasePedestrianClear INTEGER,
phaseMinimumGreen   INTEGER,
phasePassage        INTEGER,
phaseMaximum1       INTEGER,
phaseMaximum2       INTEGER,
phaseYellowChange   INTEGER,
phaseRedClear       INTEGER,
phaseRedRevert      INTEGER,
phaseAddedInitial   INTEGER,
phaseMaximumInitial INTEGER,
phaseDynamicMaxLimit INTEGER,
phaseDynamicMaxStep INTEGER,
phaseOptions        INTEGER,
phaseRing           INTEGER,
phaseConcurrency    OCTET STRING,
phaseMaximum3       INTEGER,
phaseYellowandRedChangeTimeBeforeEndPedClear INTEGER,
phasePedWalkService INTEGER,
phaseDontWalkRevert INTEGER,
phasePedAlternateClearance INTEGER,
phasePedAlternateWalk INTEGER,
phasePedAdvanceWalkTime INTEGER,
phasePedDelayTime   INTEGER,
phaseAdvWarnGrnStartTime INTEGER,
```

phaseAdvWarnRedStartTime INTEGER,
phaseAltMinTimeTransition INTEGER }

phaseOptions OBJECT-TYPE

PhaseStatusGroupEntry
PhaseControlGroupEntry

Per Unit Parameters
Startup Flash Parameter
Automatic Ped Clear Parameter
Unit Red Revert Parameter

unitFlashStatus OBJECT-TYPE
SYNTAX INTEGER { other(1),
notFlash(2),
automatic(3),
localManual(4),
faultMonitor(5),
mmu(6),
startup(7),
preempt (8)}

unitAlarmStatus2 OBJECT-TYPE

Bit 5: Offset Transitioning - Whenever the CU is performing an offset transition (correction in process)
Bit 4: Stop Time - When either CU Stop Time Input becomes active.
Bit 3: External Start - When the CU External Start becomes active.

unitAlarmStatus1 OBJECT-TYPE

Bit 7: CoordActive - When coordination is active and not preempted or overridden.
Bit 6: Local Free - When any of the CU inputs and/or programming cause it not to run coordination.
Bit 5: Local Flash - When the Controller Unit Local Flash input becomes active, MMU Flash input is not active, and Flash is not commanded by the system.
Bit 4: MMU Flash - When the Controller Unit MMU Flash input remains active for a period of time exceeding the Start-Up Flash time.

shortAlarmStatus OBJECT-TYPE

Bit 1: T&F Flash - When either the Local Flash or MMU Flash input becomes active.
Bit 0: Preempt - When any of the CU Preempt inputs become active.

unitControl OBJECT-TYPE

Bit 5: Walk Rest Modifier
Bit 4: Call to Non-Actuated 2
Bit 3: Call to Non-Actuated 1
Bit 2: External Minimum Recall -

MCE / Manual Advance

Startup Flash

PreemptEntry ::= SEQUENCE {

RingControlGroupEntry ::= SEQUENCE {
Channel Movement Type
channelGreenType OBJECT-TYPE
SYNTAX INTEGER { other (1),

```
protected (2),
permissive (3),
flashYellow (4),
flashRed (5) }
OverlapEntry ::= SEQUENCE
```

A.6 TSCBM and SPaT Data

This section provides additional guidance if the Traffic Signal Controller Broadcast Message (TSCBM) is exchanged between the TSC infrastructure and the RSU to generate a SPaT message.

NTCIP 1202 v02 did not address the interface between the ASC and the RSU. Therefore, the TSCBM, defined in Section 3 in the V2I Hub ICD, was developed to complement NTCIP 1202 v02 for early connected vehicle pilots. The information in the TSCBM from the ASC was used by RSUs in addition to NTCIP 1202 v02 data to generate SPaT messages. See G.2.4 TSCBM for additional notes on using the TSCBM.

Table 8 describes the sources for each of the data frames and data elements that comprise the SPaT message broadcasted by the RSU based on how the connected intersection is configured and what SPaT information message is used between the TSC infrastructure and the RSU. Three potential SPaT information messages were identified in the CI Implementation Guide, the SAE J2735 SPaT Message, NTCIP 1202 v03A, and the TSCBM. However, since the CI Committee does not recommend deploying TSCBM at new locations, Table 8 did not include the source of the data frames and data elements for the SPaT message when using the TSCBM.

However, since most existing implementations use the TSCBM to provide information from the TSC infrastructure to the RSU, this section and Table 15 are provided for additional guidance based on the design content in the CI Implementation Guide. Similar to Table 8, Table 15 contains links to the specific sections in this CI Implementation Guide with the design details for generating that data element value, based on the UPER-encoded SPaT Message and the TSCBM.

- **SAE J2735 Data Element, Bit** column describes the data element (and bit) of interest
- **SAE J2735 SPaT Message** column is a link to a section describing that data element in more detail
- **TSCBM** column describes the byte(s) and bits within the TSCBM containing the data source for the data element (and bit) of interest
- **Notes** column contains additional information about using the TSCBM byte(s) and bits.

Table 15. Mapping of J2735 Elements to TSCBM

SAE J2735 Data Element, Bit	CTI 4501 Reference	TSCBM	Notes
timeStamp (DE_MinuteOfTheYear)	See 4.3.3.2.3	Bytes 236-240: spatTimeStamp (5 bytes, hours-minute-second-millisecond) Clock source may not be UTC.	Generated by the RSU spatTimestamp describes the time within the day when the TSCBM is generated. The RSU needs to convert this time to the Minute of the Year. The time source used to generate spatTimestamp may vary. Thus, the RSU may need to convert this time to UTC (universal time coordinate) time.
Id=DF_IntersectionReferenceID	See 4.3.3.3.1		
region=DE_RoadRegulatorID	See 4.3.3.3.1.2	Unsupported.	Defined in the RSU
id=DE_IntersectionID	See 4.3.3.3.1.3	Unsupported.	Defined in the RSU
revision=DE_MsgCount	See 4.3.3.2.2.1	Byte 234: spatDiscontinuousChangeFlag Bits 3-7	spatDiscontinuousChangeFlag is static and fixed at 0x11. Thus the binary will look like: 0b00010XXX, where XXX is variable.
status=DE_IntersectionStatusObject (manualControllsEnabled(0))	See 4.3.3.3.2.1	Byte 232: spatIntersectionStatus Bit 0: Manual Control Enable Active	Bit 0 is the MSB. 0x80 would be manual control.
status=DE_IntersectionStatusObject, stopTimelsActivated(1)	See 4.3.3.3.2.2	Byte 232: spatIntersectionStatus Bit 1: Stop Time (all rings) Active	
status=DE_IntersectionStatusObject, failureFlash(2)	See 4.3.3.3.2.3	Byte 232: spatIntersectionStatus Bit 2: Fault Flash Active	
status=DE_IntersectionStatusObject, preemptIsActive(3)	See 4.3.3.3.2.4	Byte 232: spatIntersectionStatus Bit 3: Preempt Active	
status=DE_IntersectionStatusObject, signalPriorityIsActive(4)	See 4.3.3.3.2.5	Byte 232: spatIntersectionStatus Bit 4: TSP Active	
status=DE_IntersectionStatusObject, fixedTimeOperation(5)	See 4.3.3.3.2.6	Unsupported.	
status=DE_IntersectionStatusObject, trafficDependentOperation(6)	See 4.3.3.3.2.7	Unsupported.	
status=DE_IntersectionStatusObject, standbyOperation(7)	See 4.3.3.3.2.8	Byte 232: spatIntersectionStatus Bit 7: Programmed Flash Active	
status=DE_IntersectionStatusObject, failureMode(8)	See 4.3.3.3.2.9	Unsupported.	
status=DE_IntersectionStatusObject, off(9)	See 4.3.3.3.2.10	Unsupported.	Value cannot come from the controller if it is off.

SAE J2735 Data Element, Bit	CTI 4501 Reference	TSCBM	Notes
status=DE_IntersectionStatusObject, recentMAPmessageUpdate(10)	See 4.3.3.3.2.11	Unsupported.	Generated by the RSU or is blank.
status=DE_IntersectionStatusObject, recentChangeinMAPAssignedLanesIDs Used(11)	See 4.3.3.3.2.12	Unsupported.	Generated by the RSU or is blank.
status=DE_IntersectionStatusObject, noValidMAPisAvailableAtThisTime(12)	See 4.3.3.3.2.13	Unsupported.	Generated by the RSU or is blank.
status=DE_IntersectionStatusObject, noValidSPATisAvailableAtThisTime(13)	See 4.3.3.3.2.14	Unsupported.	Generated by the RSU or is blank.
timeStamp=DE_Dsecond	See 4.3.3.2.3.2	Bytes 236-240: spatTimeStamp Clock source may not be UTC.	Generated by the RSU spatTimestamp (5 bytes, hours-minute-second-millisecond) describes the time within the day when the TSCBM is generated. The RSU needs to convert this time to milliseconds in the current UTC minute. The time source used to generate spatTimestamp may vary. Thus, the RSU may need to convert this time to UTC (universal time coordinate) time.
enabledLanes=DF_EnabledLaneList	See 4.3.3.3.7	Unsupported.	Generated by the RSU
states=DF_MovementList	See 4.3.3.3.3		
signalGroup=DE_SignalGroupID	See 4.3.3.3.3.1	Unsupported.	The RSU must provide a means to relate Vehicle, Pedestrian, and Overlap phases in the TSCBM to signal groups in the J2735 SPaT message.
state-time-speed=DF_MovementEventList			
eventState=DE_MovementPhaseState (Current Movement)	See 4.3.3.3.3	Vehicle Phases Bytes 210-211: phaseStatusGroupReds Bytes 212-213: phaseStatusGroupYellows Bytes 214-215: phaseStatusGroupGreens Vehicle Overlaps Bytes 222-223: overlapStatusGroupReds	The RSU must provide a means to configure the protected or permissive state of the signal group related to the TSCBM Vehicle, Pedestrian, or Overlap phases, including configuring a protected permissive signal group. For example, the TSCBM does not indicate if a left turn is a permitted left turn or a protected turn. The distinction is made in a (proprietary) table within the RSU and used when the RSU

SAE J2735 Data Element, Bit	CTI 4501 Reference	TSCBM	Notes
		Bytes 224-225: overlapStatusGroupYellows Bytes 226-227: overlapStatusGroupGreens Pedestrians Bytes 216-217: phaseStatusGroupDontWalks Bytes 218-219: phaseStatusGroupPedClears Bytes 220-221: phaseStatusGroupWalks	generates the SAE J2735 SPaT message for broadcast.
eventState=DE_MovementPhaseState (Next Movement)	See 4.3.3.3.4	Unsupported. Defined by vendor.	TSCBM does not support providing the next state of the movement as required by CTI 4501.
timing=DF_TimeChangeDetails	See 4.3.3.3.5		
startTime=DE_TimeMark	See 4.3.3.3.5.7, 4.3.3.3.5.8	Unsupported. Defined by vendor.	TSCBM does not support providing the start time of the next movement as required by CTI 4501.
minEndTime=DE_TimeMark	See 4.3.3.3.5.3	Vehicle Phases Byte 2: phase number Bytes 3-4: spatVehMinTimeToChange Up to 16 phases are supported in bytes in 2-209. Vehicle Overlaps Byte 2: phase number Bytes 11-12: spatOvlpMinTimeToChange Up to 16 overlaps are supported in bytes in 2-209. Pedestrians Byte 2: phase number Bytes 7-8: spatPedMinTimeToChange Up to 16 phases are supported in bytes in 2-209.	Generated by the RSU The TSCBM was developed based the 2009 version of SAE J2735 (SAE J2735_200911), where DE_TimeMark indicates how much time remains before an event occurs. The 2015 version (SAE J2735_201509) updated DE_TimeMark to indicate the time within the hour at which a signal phase is expected to change. Thus, the RSU must convert the time to change in the TSCBM to time of change in the J2735 SPaT message.
maxEndTime=DE_TimeMark	See 4.3.3.3.5.4	Vehicle Phases Byte 2: phase number	Generated by the RSU

SAE J2735 Data Element, Bit	CTI 4501 Reference	TSCBM	Notes
		<p>Bytes 5-6: spatVehMaxTimeToChange Up to 16 phases are supported in bytes in 2-209.</p> <p>Vehicle Overlaps Byte 2: phase number Bytes 12-13: spatOvlpMaxTimeToChange Up to 16 overlaps are supported in bytes in 2-209.</p> <p>Pedestrians Byte 2: phase number Bytes 9-10: spatPedMaxTimeToChange Up to 16 phases are supported in bytes in 2-209.</p>	<p>The TSCBM was developed based the 2009 version of SAE J2735 (SAE J2735_200911), where DE_TimeMark indicates how much time remains before an event occurs. The 2015 version (SAE J2735_201509) updated DE_TimeMark to indicate the time within the hour at which a signal phase is expected to change. Thus, the RSU must convert the time to change in the TSCBM to time of change in the J2735 SPaT message.</p>
nextTime=DE_TimeMark	See 4.3.3.3.6.1	Unsupported. Defined by vendor.	TSCBM does not support providing the time of the next allowed movement as required by CTI 4501.

Defined in the RSU = indicates the value is input into the RSU and not calculated.

Generated by the RSU = indicates the value is calculated by the RSU, possibly via a lookup table.

A.7 Latency and Timing Error Analysis for Connected Intersections

A.7.1 Latency

The Red Light Violation Warning (RLVW) application described in Section 2.6.1 of the CI Implementation Guide has been a catalyst for discovering new needs and requirements for connected intersections. In a non-connected environment, human drivers and highly automated vehicles depend on the displayed signal indications as the method of communication from the signal system. In a CI environment, however, information flow takes two different pathways to convey signal phase information to the driver. As shown in Figure 39, a Traffic Signal Controller (TSC) generates new signal state information every tenth of second (10 Hz Processing Loop). Pathway #1 illustrates TSC issuing commands over the field cabinet system's communications bus to activate the appropriate signal indications. Pathway #2 illustrates TSC transmitting the corresponding SPaT information through an Ethernet connection for processing and transmission (usually performed in a RSU over-the-air to CVs).

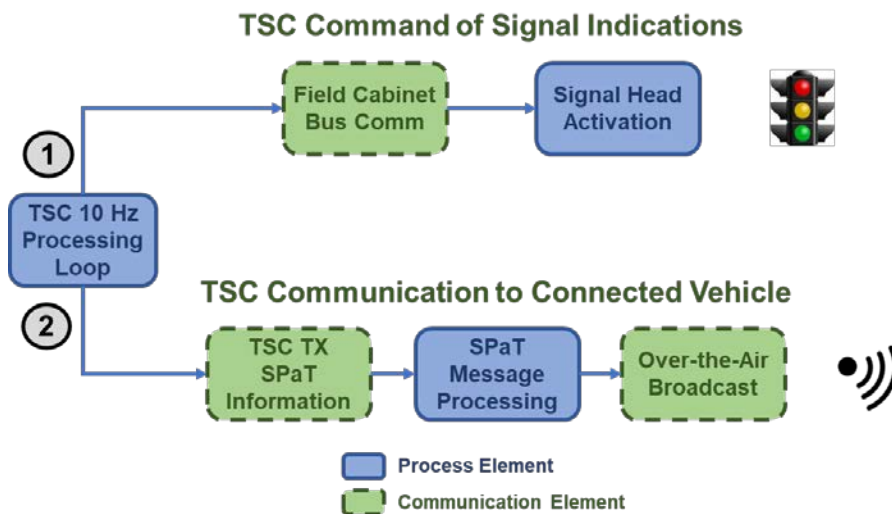


Figure 39. Flow of Roadway Information in a Connected Intersection.

The RLVW application in a CV generates advisories, warnings, or alerts based on the received SPaT information and the vehicle dynamics to allow a driver to take appropriate action. To be safe and effective, it is important that the visual indication provided in Pathway #1 and the SPaT information provided in Pathway #2 are congruent in the information generation time interval, the phase activation time, and the duration of the signal state in order to avoid confusion or ambiguity to the driver. Delay in either pathway for providing the information could result in an unsafe driving condition. For instance, a vehicle traveling at 45 mph (72.5 kph) travels 66 ft (20 meters) in one second.

Latency includes delays due to information processing, including security signing and verification, V2X, and Ethernet interface latency (medium access plus propagation delay), and Cabinet Data Bus Latency:

Pathway #1 Latency = Information Processing Time + Cabinet Data Bus Communications Latency

Pathway #2 Latency = Information Processing Time + V2X and Ethernet Interface Latency

Where:

- Information Processing Time is the delay associated with generating SPaT. For example, the amount of processing time to generate the UPER-encoded SPaT message. This delay also includes security signing and verification. The information processing by the TSC is not included

in the estimates because it occurs inside the TSC 10 Hz Processing Loop before the start of the two pathways.

- V2X and Ethernet Interface Latency is the delay associated with communicating the intended information over the communication link using the specified protocol. This delay includes the amount of time waiting for a scheduled transmit opportunity over the Ethernet interface between the TSC and RSU, as well as the over-the-air (OTA) interface between RSU and vehicle.
- Cabinet Data Bus Communications Latency is the delay associated with communicating the intended information over the field cabinet system's serial data bus.

These latencies can be calculated for both pathways shown in Figure 39. Table 16 lists estimated maximum latencies for Pathway #1 from the TSC to signal activation. They are provided for discussion, testing, and agreement with stakeholders. In the case of the Field Cabinet Bus Communications, there was a range of 100 ms to 220 ms. For purposes of this discussion, 220 ms will be used.

Table 16. Example Maximum Latencies for Pathway #1 from the TSC to signal activation.

Description	Time (milliseconds)
Field Cabinet Bus Communications	
<ul style="list-style-type: none"> • High-level Data Link Control (HDLC) using Serial Interface Units (SIUs) - or - • Synchronous Data Link Control (SDLC) using Bus Interface Units (BIUs) 	220
Signal Head Activation	
<ul style="list-style-type: none"> • Time to turn on the signal light (includes time taken by switch packs) 	30
Total	250

Table 17 lists estimated maximum latencies for Pathway #2 from the TSC to the OTA broadcast of the SPaT message. They are provided for discussion, testing, and agreement with stakeholders.

Table 17. Example Maximum Latencies for Pathway #2 from the TSC to the OTA Broadcast of the SPaT Message.

Description	Time (milliseconds)
TSC Transmission of SPaT Information to RSU	
<ul style="list-style-type: none"> • Ethernet communication of NTCIP/TSCBM SPaT information 	10
SPaT Message Processing	
<ul style="list-style-type: none"> • Generate UPER encoded SPaT message per SAE J2735 • Process SPaT message for appropriate SCMS security for message broadcast 	30
Over-the-Air Message Broadcast	60 +/- 10 ⁷
Total	115 ± 10

Since it is the desire for the latency of the two pathways to be the same, then an allowable latency difference (ALD) between the two pathways needs to be established. It is likely that each application on the CV that uses CI information may have a different ALD for which it can be effective. For the RLVW application, it has been proposed that the ALD is 200 ms. The ALD is not a norm and it is assumed that the systems are able to maintain the 100 ms SPaT message interval. Computing the maximum latency estimates from Table 16 and Table 17, the expected latency difference will be the absolute value of the difference in latencies of Pathway #1 and Pathway #2 or:

⁷ Communication delay depends on the medium used. In the case of CV2X and a packet delay budget of 50 ms, with HARQ set to on, the information is expected to be delivered within 60 to 70 ms. This delay could be further optimized/reduced with more predictable periodicity of the SPAT message being sent from controller to RSU.

$$| 250 \text{ ms} - 130 \text{ ms} | = 120 \text{ ms}$$

which is below the 200 ms ALD.

The values in Table 16 and Table 17 are estimates and should be validated through testing, then adjusted accordingly. In this analysis, it is assumed that the TSC begins both pathways nearly simultaneously inside the TSC. If testing identifies a significant time difference in starting the two pathways, then an additional latency could be added to the calculations.

Recommendations are as follows:

- a) The latencies in Table 16 and Table 17 should be tested to validate the estimates.
- b) It is essential that all the of the subsystems maintain UTC time. It is recommended that the real-time clock of the TSC be maintained by using Network Time Protocol (NTP) and with the RSU as the NTP server. The Advanced Transportation Controller (ATC) Standard already requires NTP on ATC units and the RSU Standard is being updated to require that RSUs be able to act as NTP servers.
- c) ITS standards for field cabinet systems need to be updated to tighten tolerances and reduce latency variability for both Pathway #1 and Pathway #2.
- d) The ATC Application Programming Interface (API) Standard and the open source software API Reference Implementation (APIRI) should be updated to perform the transmission of the SPaT information to the RSU. API software runs on ATC units and already handles communications on the cabinet communication bus. Using this “middleware” to also perform the SPaT message transmission would provide more control between the two paths and the software could potentially compensate for larger variances in latencies occurring between the two pathways. This recommendation came from the TSC manufacturers to reduce latency and have more consistent operation across manufacturers.
- e) Agencies should procure ATC units with more powerful processors and more memory. Also, ATC units are built using an ATC “Engine Board.” Underpowered ATC units can be updated by replacing the existing engine board with a more capable one.

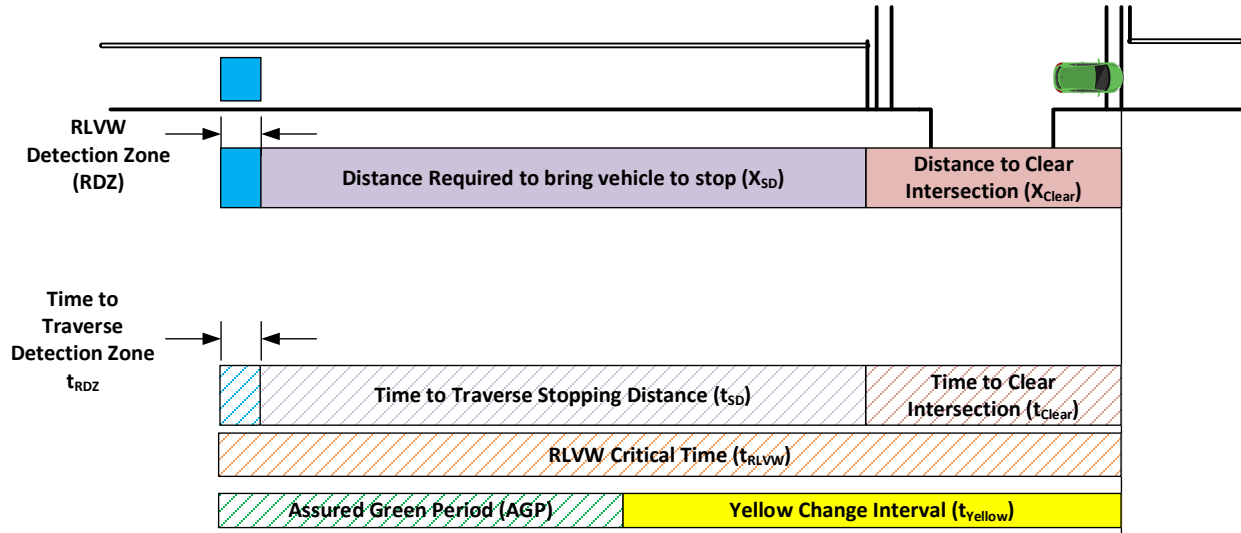
A.7.2 Timing Error

In addition to latency, the accuracy of the TSC’s or the RSU’s UTC estimate used to timestamp the SPaT data may introduce additional performance challenges that relate to latency. One source of timestamp error is the difference between UTC and the TSC’s estimate of UTC. The error in this estimate may be exacerbated by TSC processing delays, so the overall communication range and the length of the assured green period may need to be further optimized to compensate for timing error. Future revisions of this document may provide more guidance on how to compensate for errors in UTC estimates.

Annex B Assured Green Period Use Cases [Informative]

B.1 Background Information

This Annex provides some example use cases for calculating the Assured Green Period.



Assumptions for illustrative purposes ONLY:

- Maximum Reception ranges of DSRC Unit ($X_{RSURange}$) = 1000 ft
- Distance to Clear Intersection = 150 ft
- Approach Speed ($V_{Approach}$) = 50 mph or 75 ft/s (rounded up for simplification of computations)
- Intersection Clearance Distance (X_{Clear}) = 150 ft
- Yellow change interval (t_{Yellow}) = 5 second (*MUTCD* permits range from 3 to 6). NOTE: The yellow time should be calculated using accepted engineering practices - 5 seconds is used here only as an example for the purpose of this illustration.
- Perception/Reaction Time ($t_{P/R}$) = 1 second
- Stopping Deceleration Rate (a) = 10 ft/s²
- Detection Time (t_{RDZ}) = 0.5 sec (assumed maximum)
- No all red time ($AR = 0$ sec)
- Vehicle does not begin to decelerate before onset of yellow

Base Calculations

- RLVW Detection Zone (RDZ)

$$RDZ = t_{RDZ} * V_{Approach} = 0.5 \text{ sec} * 75 \text{ ft/s} = 37.5 \text{ ft}$$

- Stopping Distance (Basic Kinematic Equation)

$$X_{SD} = V_{Approach} t_{P/R} + \frac{-V_{Approach}^2}{2(a \pm Gg)} = 75 \text{ ft/s}(1\text{s}) - \frac{-(75 \text{ ft/s})^2}{2(-10 \text{ ft/s}^2 \pm 0)} = 356.25 \text{ ft}$$

- Time to Clear Intersection

$$t_{Clear} = \frac{X_{Clear}}{V_{Approach}} = \frac{150 \text{ ft}}{75 \text{ ft/s}} = 2 \text{ sec}$$

- Time to Travel Through Stopping Distance at Approach Speed

$$t_{SD} = \frac{X_{SD}}{V_{Approach}} = \frac{356.25 \text{ ft}}{75 \text{ ft/s}} = 4.75 \text{ sec}$$

- Red Light Violation Warning Critical Time (t_{RLVW})

$$t_{RLVW} = t_{SD} + t_{Clear} + t_{RDZ} = 4.75 \text{ sec} + 2 \text{ sec} + 0.5 \text{ sec} = 7.25 \text{ sec}$$

- Assured Green Period (AGP)

$$AGP = t_{RLVW} - t_{Yellow} = 7.25 \text{ sec} - 5 \text{ sec} = 2.25 \text{ sec}$$

- Distance traveled by vehicle during AGP (maintaining approach speed)

$$X_{AGP} = V_{Approach} * AGP = 75 \text{ ft/s} * 2.25 \text{ sec} = 168.75 \text{ ft}$$

- Distance traveled during Yellow Change Interval

$$X_{Yellow} = V_{Approach} * t_{Yellow} = 75 \text{ ft/s} * 5 \text{ sec} = 375 \text{ ft}$$

- Distance from RSU Reception Range to Leading Edge of RLVW Detection Zone ($X_{RSUtoRDZ}$)

$$X_{RSUtoRDZ} = X_{RSURange} - (X_{SD} + RDZ) = 1000 \text{ ft} - (356.25 \text{ ft} + 37.5 \text{ ft}) = 606.25 \text{ ft}$$

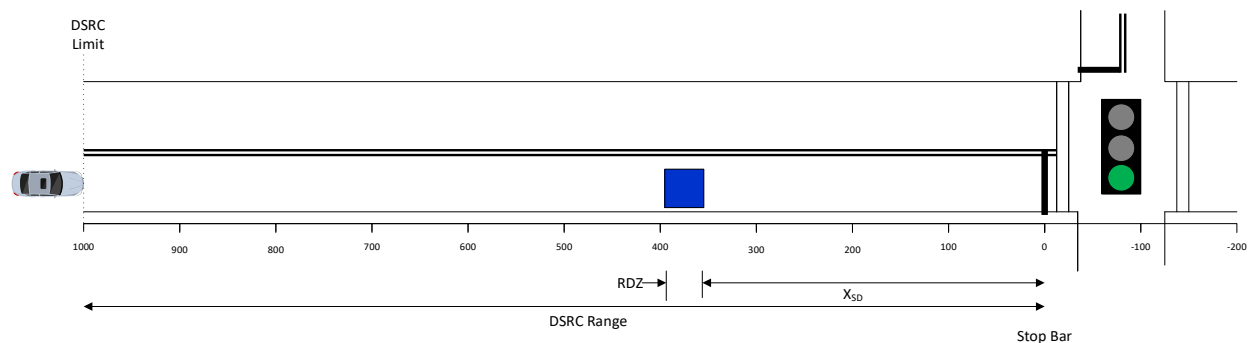
B.2 Example Use Case 1

B.2.1 No Call on Cross-Street

Traffic signal is resting in green on main street approach. A connected vehicle enters in DSRC range traveling at the Approach Speed. **The traffic signal control DOES NOT receive a call for service on a cross street approach.** For ease of calculations, the CV enters DRSC range at exactly the beginning of the hour. All times are reported as timestamps from top of hour.

Vehicle enters DSRC range at exactly top of hour ($t=0$)

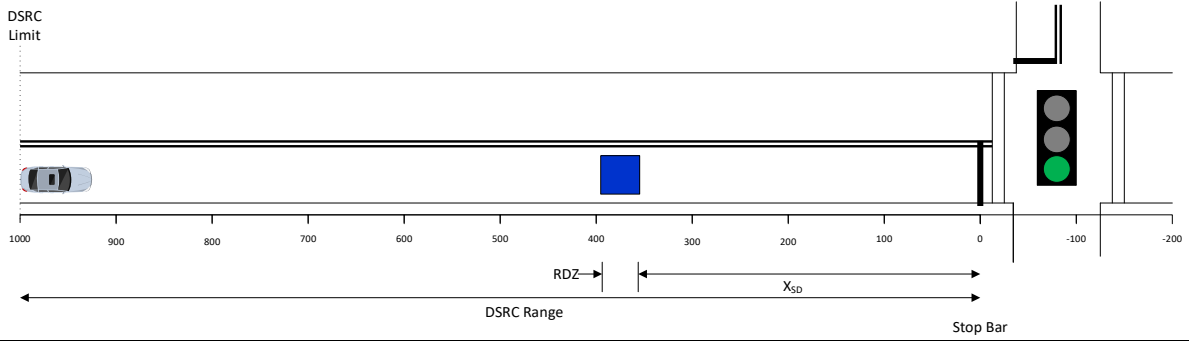
- No call on cross street



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00000	0	1000	75	Green	-	00001	36111

$t=1$ seconds after vehicle enters DSRC range

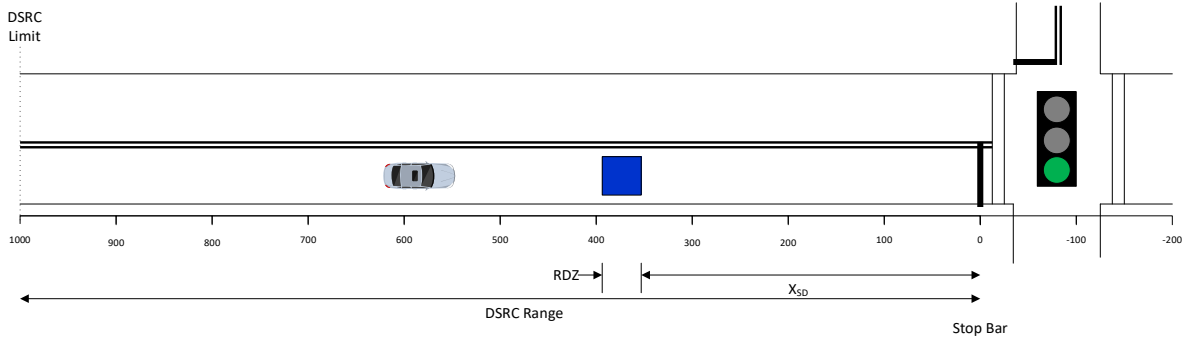
- Vehicle has traveled 75 ft since entering DSRC range
- No call on cross street



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00010	75	925	75	Green	-	00011	36111

t=6 seconds after vehicle enters DSRC range

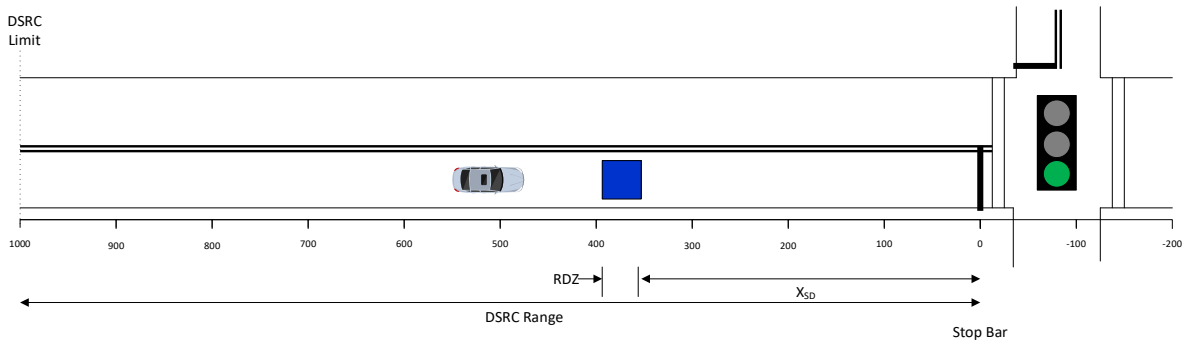
- Vehicle has traveled 450 ft since entering DSRC range
- No call on cross street



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00060	450	550	75	Green	-	00061	36111

t=7 seconds after vehicle enters DSRC range

- Vehicle has traveled 525 ft since entering DSRC range
- No call on cross street

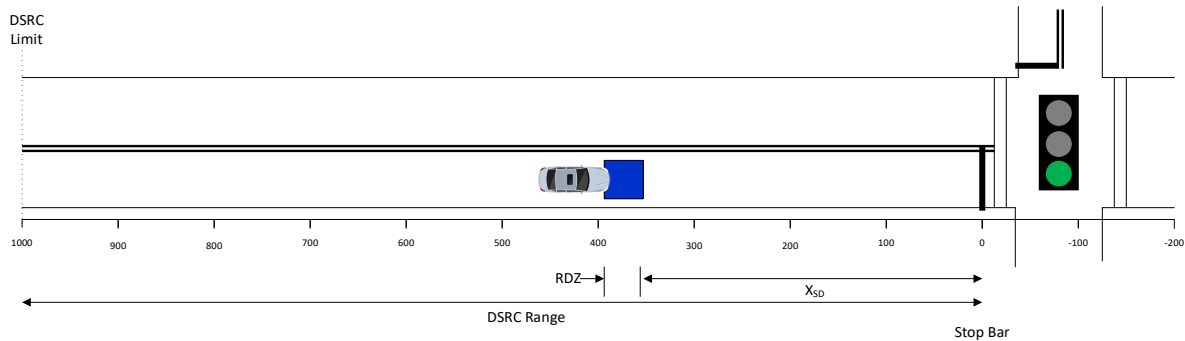


Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)

00070	525	475	75	Green	-	00071	36111
-------	-----	-----	----	-------	---	-------	-------

t=8.1 seconds after vehicle enters DSRC range

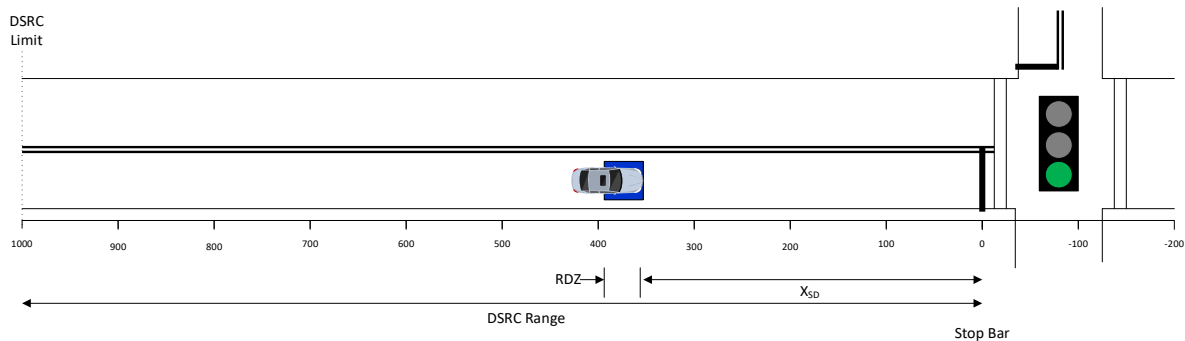
- Vehicle enters RDZ but has not be registered by controller
- No call on cross street



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00081	607.5	392.5	75	Green	-	00082	36111

t=8.5 seconds after vehicle enters DSRC range

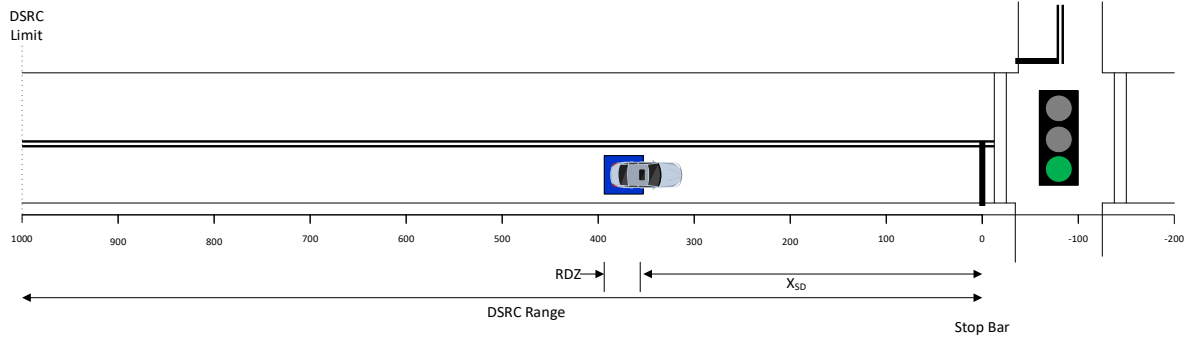
- Controller registers call in RDZ and applies the AGP
- No call on cross street



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00085	637.5	362.5	75	Green	2.3	00108	36111

t=9.0 seconds after vehicle enters DSRC range

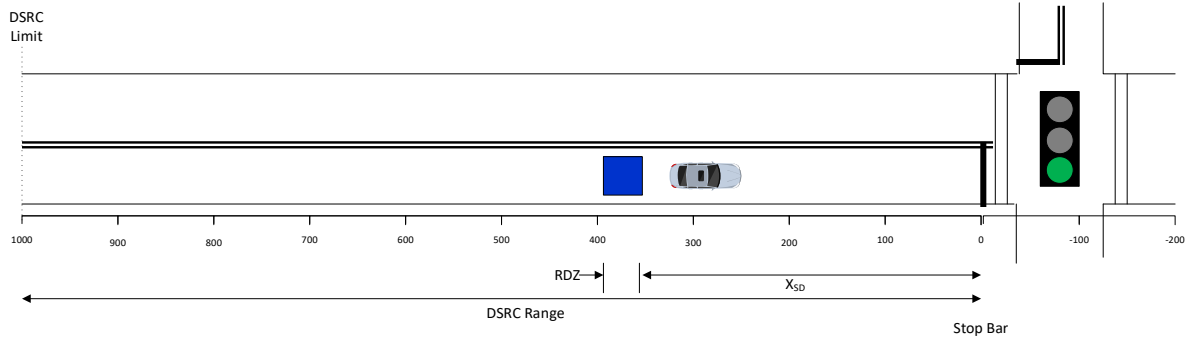
- 0.5 seconds of APG has expired
- No Call on cross-street



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00090	675	325	75	Green	1.8	00108	36111

t=10.0 seconds after vehicle enters DSRC range

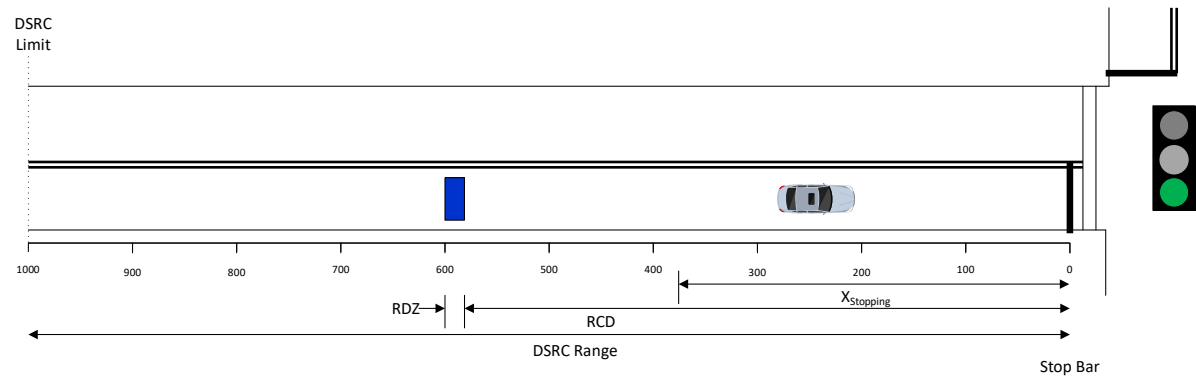
- 1.5 seconds of AGP has expired
- No Call on cross-street



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00100	750	250	75	Green	0.8	00108	36111

t= 10.8 seconds after vehicle enters DSRC range

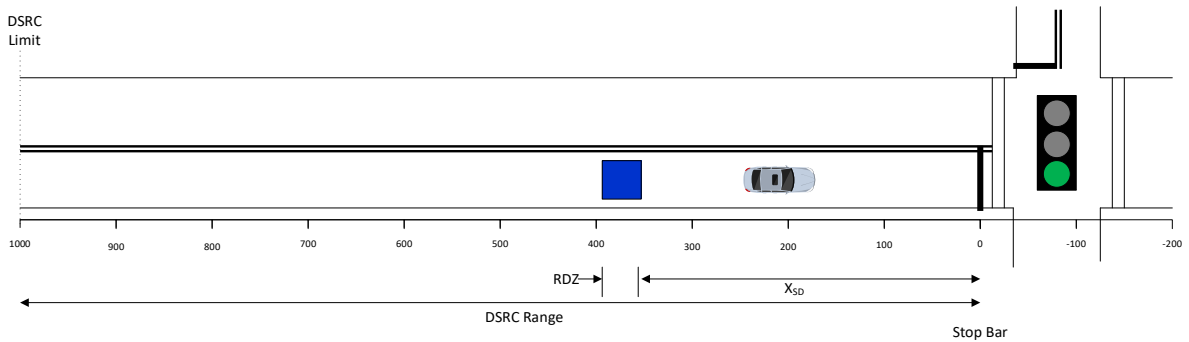
- AGP has expired
- No call on cross street



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00108	810	190	75	Green	-	00109	36111

$t=11.0$ seconds after vehicle enters DSRC range

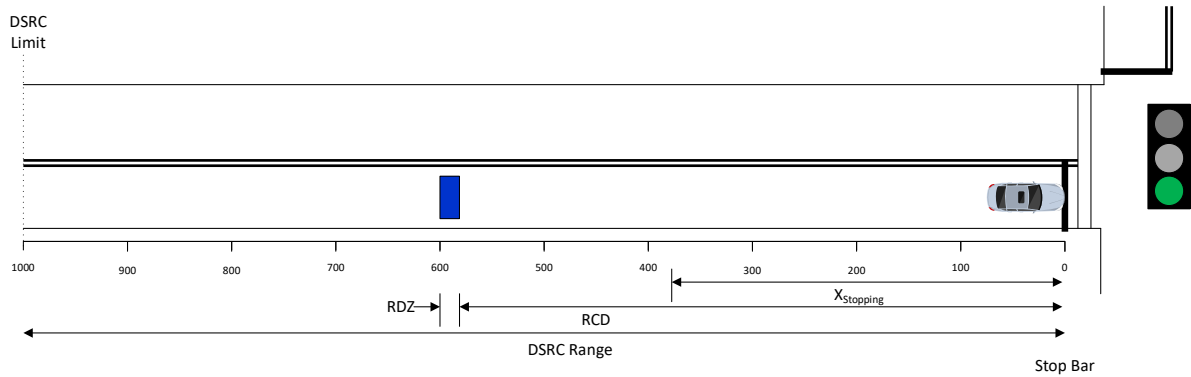
- No call on cross street



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00110	825	175	75	Green	-	00111	36111

$t=13.4$ seconds after vehicle enters DSRC range

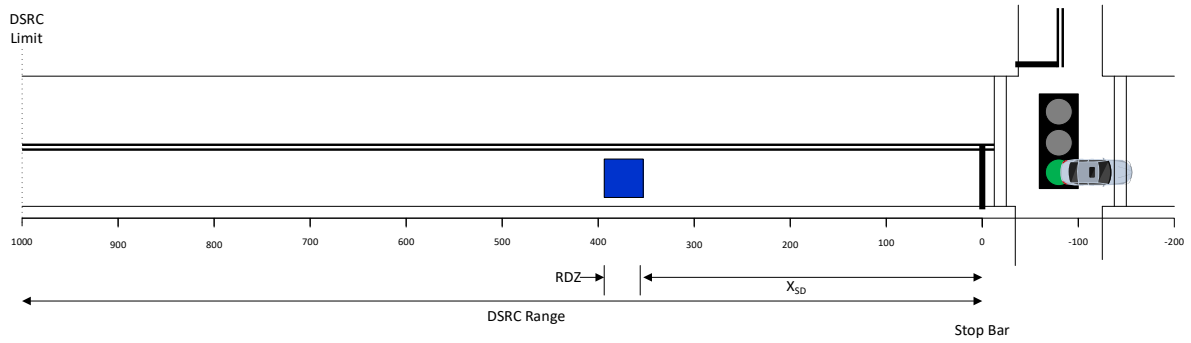
- Vehicle reaches stop line



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00134	1005	-5	75	Green	-	00135	36111

15.4 seconds after vehicle enters DSRC range ($t=15.3$)

- Vehicle clears intersection



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00154	1155	-155	75	Green	-	00155	36111

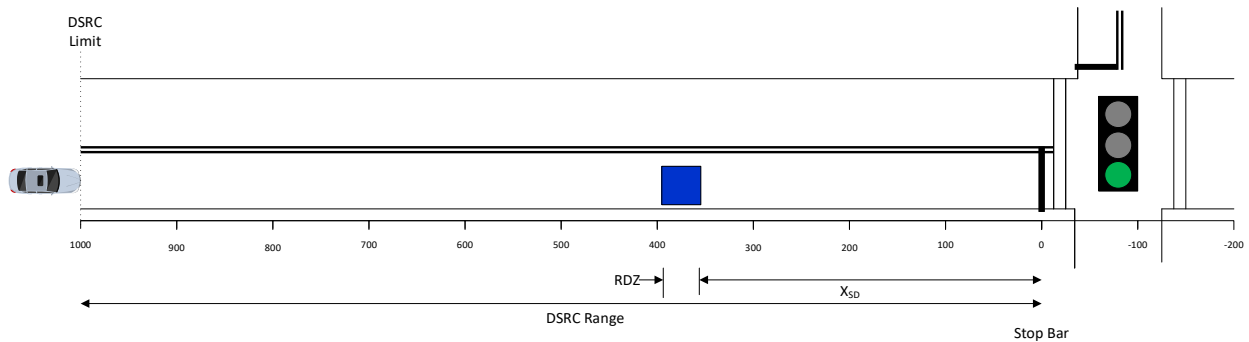
Summary

No Call on Cross-Street									
Seconds from RSU Entry	Current Timemark	Distance From RSU Range	Distance to Stop Bar	Vehicle Speed (fps)	Signal Status	time to change Remaining	minEndTime	maxEndTime	
0	00000	0	1000	75	Green	0.1	00001	36111	
1	00010	75	925	75	Green	0.1	00011	36111	
6	00060	450	550	75	Green	0.1	00061	36111	
7	00070	525	475	75	Green	0.1	00071	36111	
7.5	00075	562.5	437.5	75	Green	0.1	00076	36111	
8	00080	600	400	75	Green	0.1	00081	36111	
8.1	00081	607.5	392.5	75	Green	0.1	00082	36111	Vehicle in RDZ
8.5	00085	637.5	362.5	75	Green	2.3	00108	36111	Controller applies AGP
9	00090	675	325	75	Green	1.8	00108	36111	
10	00100	750	250	75	Green	0.8	00108	36111	
10.8	00103	810	190	75	Green	0.1	00109	36111	
11	00110	825	175	75	Green	0.1	00111	36111	
12	00120	900	100	75	Green	0.1	00121	36111	
13	00130	975	25	75	Green	0.1	00131	36111	
13.4	00134	1005	-5	75	Green	0.1	00131	36111	Vehicle reaches stop bar
14	00140	1050	-50	75	Green	0.1	00141	36111	
15	00150	1125	-125	75	Green	0.1	00151	36111	
15.4	00153	1155	-155	75	Green	0.1	00155	36111	Vehicle clears Intersection

B.2.2 Call on Cross-Street at t=9

Traffic signal is resting in green on mainstreet approach. A connected vehicle enters in DSRC range traveling at the Approach Speed. **Nine seconds after entering DSRC range, the traffic signal control receives a call for service on a cross-street approach.** For ease of calculations, the CV enters DSRC range at exactly the beginning of the hour. All times are reported as timestamps from top of hour. Vehicle enters DSRC range at exactly top of hour (t=0)

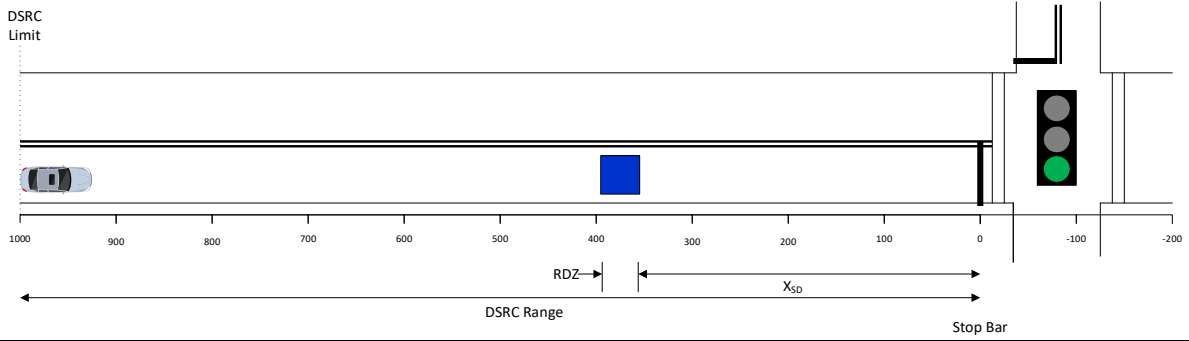
- No call on cross street



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00000	0	1000	75	Green	-	00001	36111

t=1 seconds after vehicle enters DSRC range

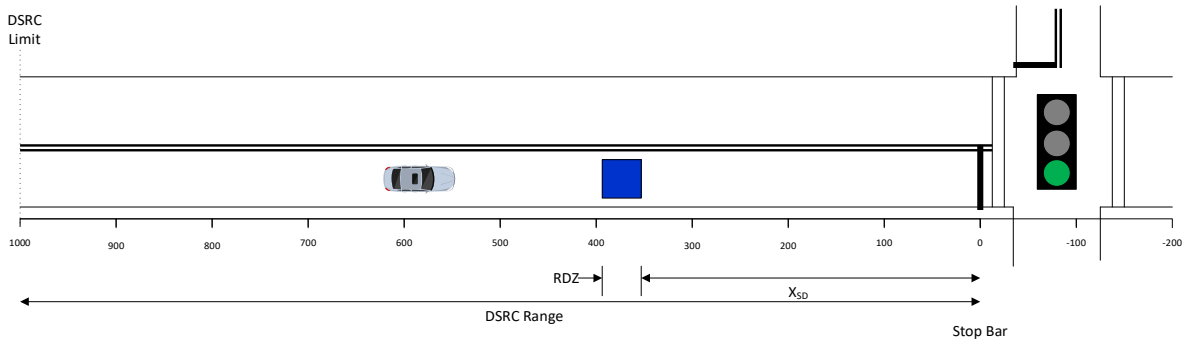
- Vehicle has traveled 75 ft. since entering DSRC range
- No call on cross street



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00010	75	925	75	Green	-	00011	36111

t=6 seconds after vehicle enters DSRC range

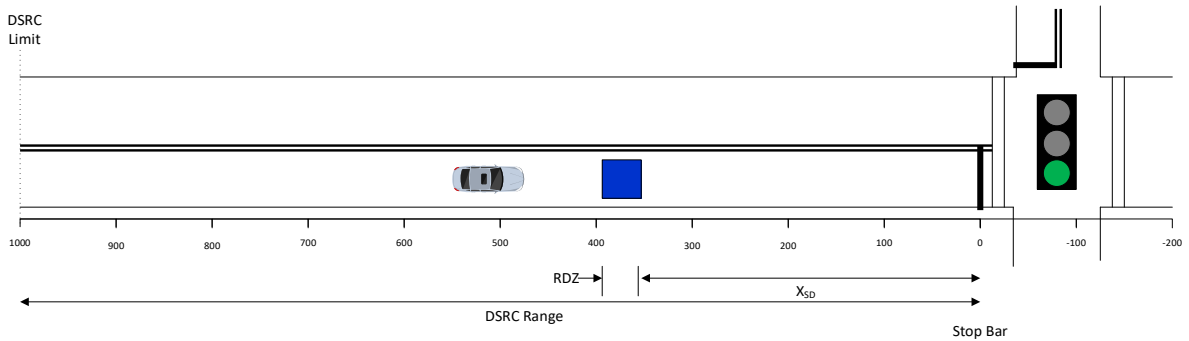
- Vehicle has traveled 450 ft. since entering DSRC range
- No call on cross street



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00060	450	550	75	Green	-	00061	36111

t=7 seconds after vehicle enters DSRC range

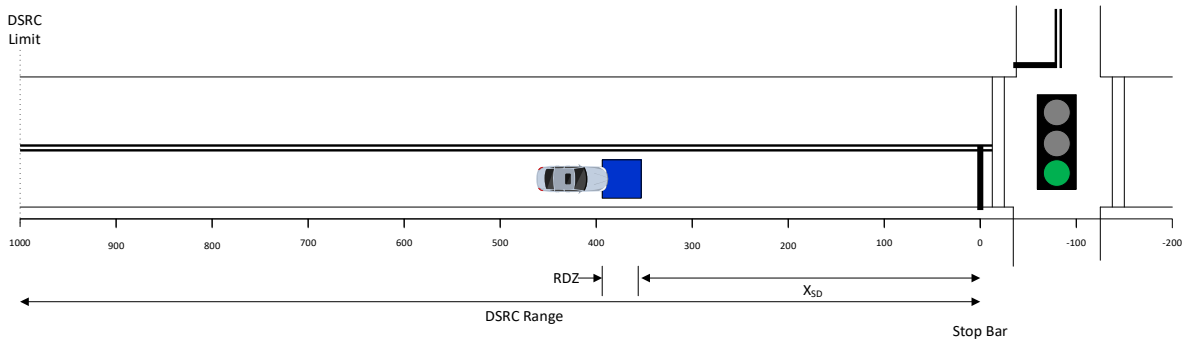
- Vehicle has traveled 525 ft. since entering DSRC range
- No call on cross street



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00070	525	475	75	Green	-	00071	36111

t=8.1 seconds after vehicle enters DSRC range

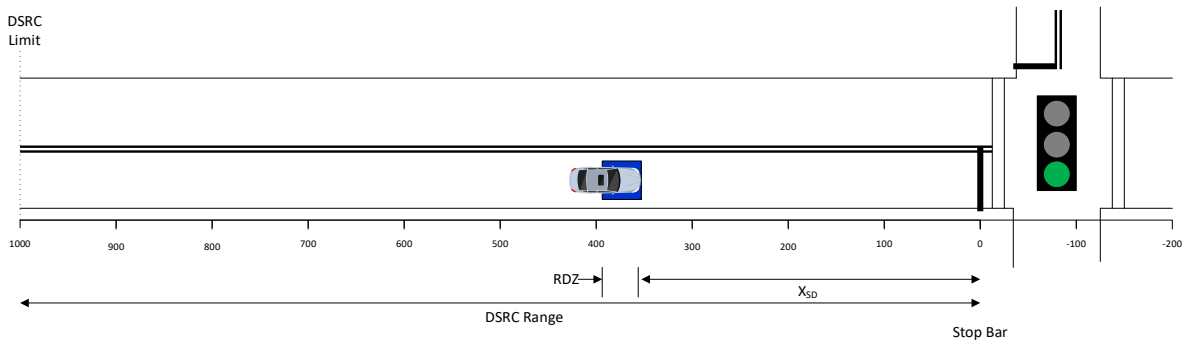
- Vehicle enters RDZ but has not be registered by controller
- No call on cross street



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00081	607.5	392.5	75	Green	-	00082	36111

t=8.5 seconds after vehicle enters DSRC range

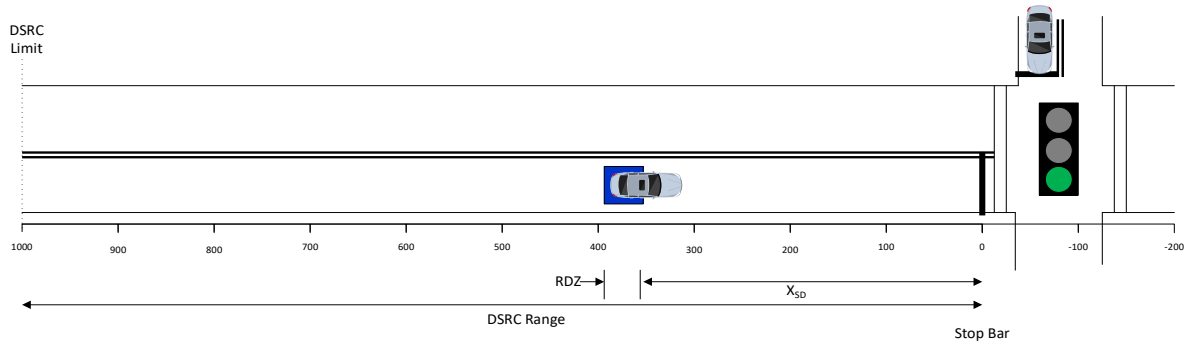
- Controller registers call in RDZ and applies the AGP
- No call on cross street



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00085	637.5	362.5	75	Green	2.3	00108	36111

t=9.0 seconds after vehicle enters DSRC range

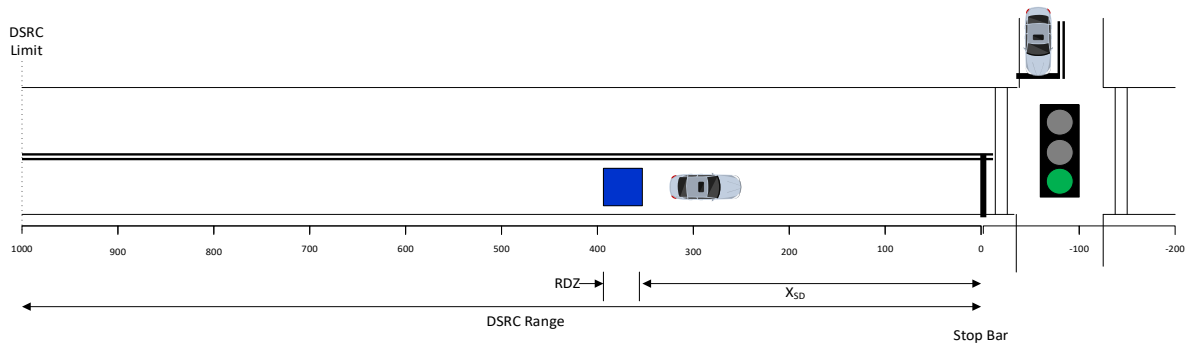
- 0.5 seconds of APG has expired
- Controller registers call on cross-street
- Sets Assured Green End Time (minEndTime = maxEndTime)



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00090	675	325	75	Green	1.8	00108	00108

t=10.0 seconds after vehicle enters DSRC range

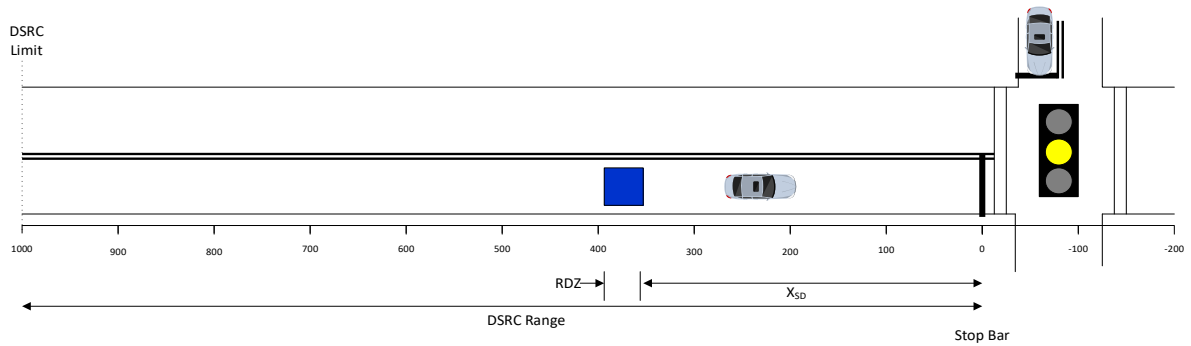
- 1.5 seconds of APG has expired
- Call registered on cross street



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00100	750	250	75	Green	0.8	00108	00108

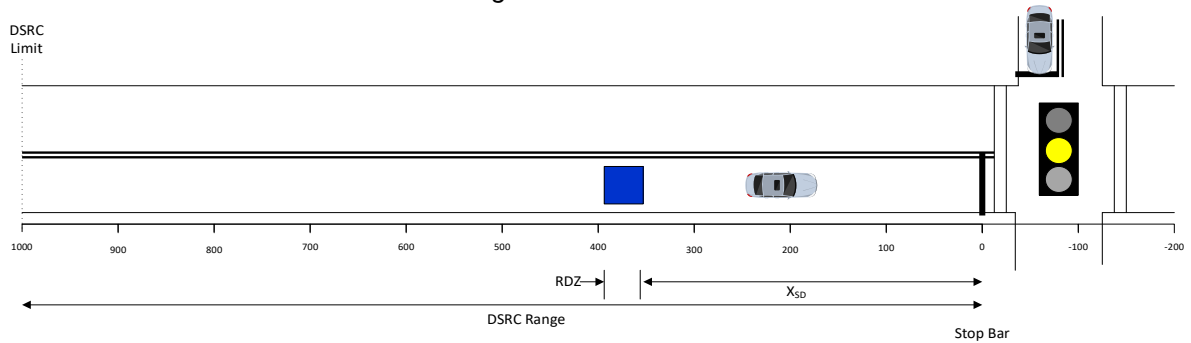
t= 10.8 seconds after vehicle enters DSRC range

- AGP has expired
- Signal transitions to yellow



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00108	810	190	75	Yellow	-	00158	00158

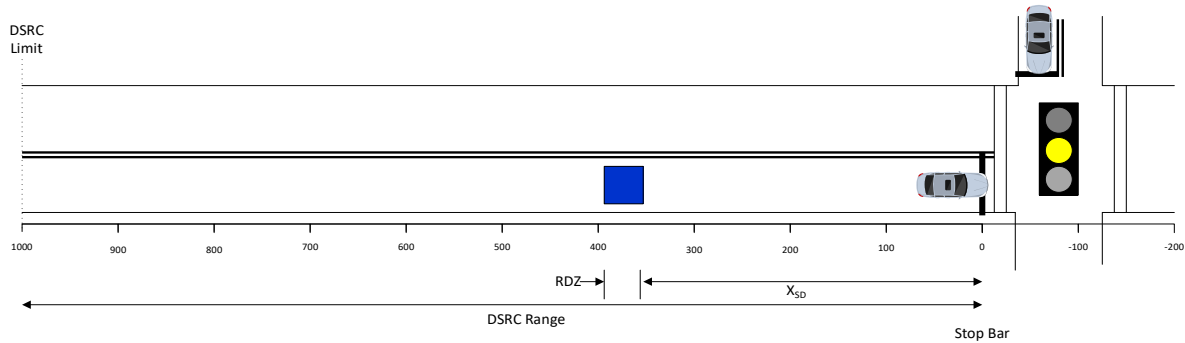
t=11.0 seconds after vehicle enters DSRC range



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00110	825	175	75	Yellow	-	00158	00158

$t=13.4$ seconds after vehicle enters DSRC range

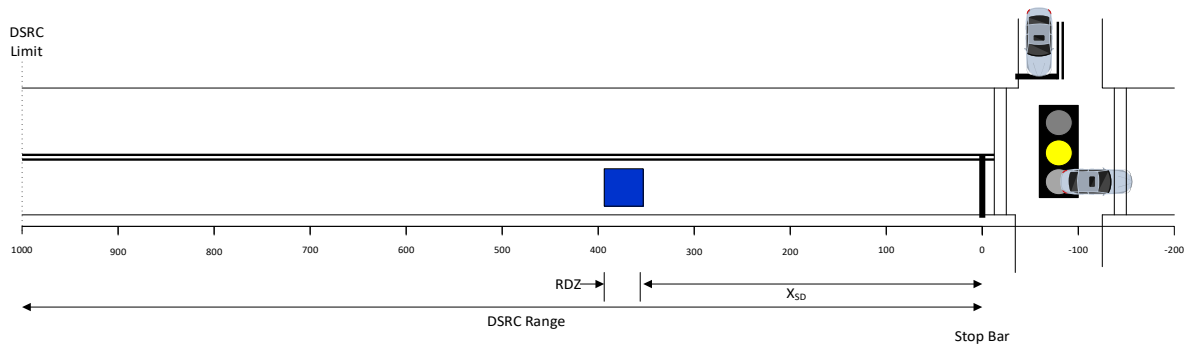
- Vehicle reaches stop line



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00134	1005	-5	75	Yellow	-	00158	00158

$t=15.4$ seconds after vehicle enters DSRC range

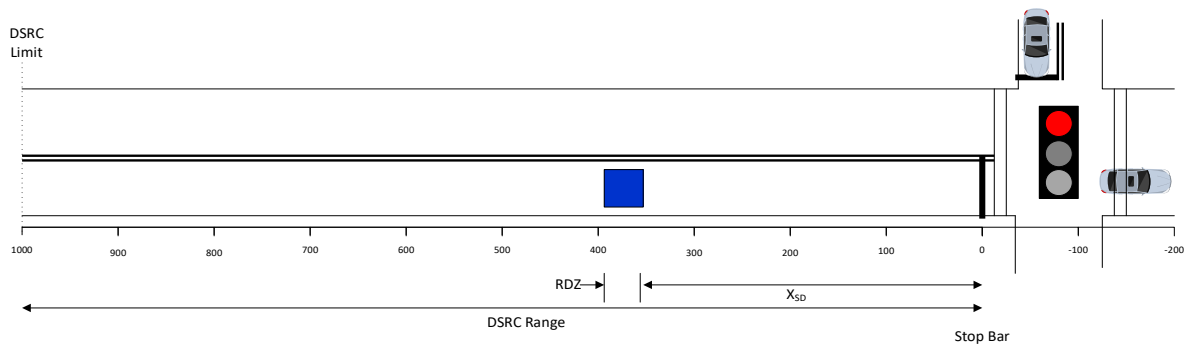
- Vehicle clears intersection



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00154	1155	-155	75	Yellow	-	00158	00158

$t=15.8$ seconds after vehicle enters DSRC range

- Signal transitions to red
- Vehicle is located -185 ft downstream of stop line



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00158	1155	-155	75	Red	-		

Summary

Call on Cross-Street @ t=9 (Vehicle to Pass Through)

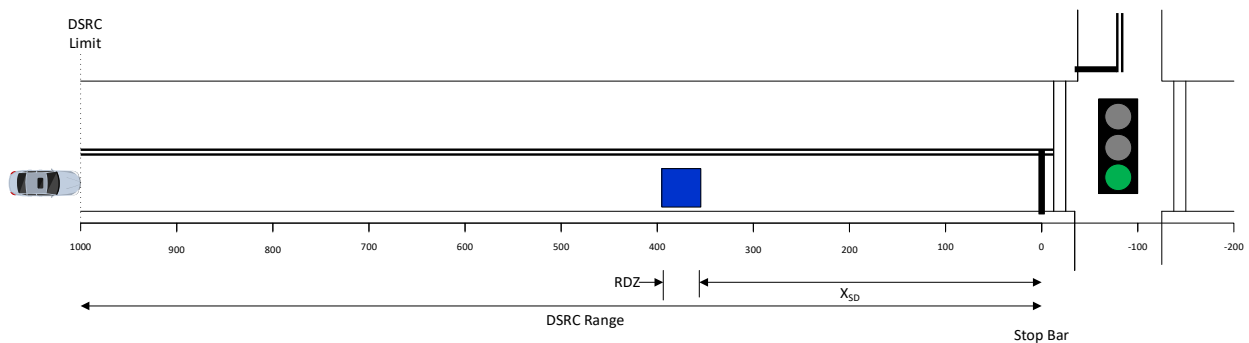
Seconds from RSU Entry	Current Timemark	Distance From RSU Range	Distance to Stop Bar	Vehicle Speed (fps)	Signal Status	time to change Remaining	minEndTime	maxEndTime	
0	00000	0	1000	75	Green	0.1	00001	36111	
1	00010	75	925	75	Green	0.1	00011	36111	
6	00060	450	550	75	Green	0.1	00061	36111	
7	00070	525	475	75	Green	0.1	00071	36111	
8	00080	600	400	75	Green	0.1	00081	36111	
8.1	00081	607.5	392.5	75	Green	0.1	00082	36111	Vehicle in RDZ
8.5	00085	637.5	362.5	75	Green	2.3	00108	36111	AGP Applied
9	00090	675	325	75	Green	1.8	00108	00108	Controller sets AGET
10	00100	750	250	75	Green	0.8	00108	00108	
10.8	00108	810	190	75	Yellow	5	00158	00158	
11	00118	825	175	75	Yellow	4.8	00158	00158	
12	00128	900	100	75	Yellow	3.8	00158	00158	
13	00130	975	25	75	Yellow	2.8	00158	00158	
13.4	00134	1005	-5	75	Yellow	2.4	00158	00158	Vehicle reaches stop Bar
14	00140	1050	-50	75	Yellow	1.8	00158	00158	Vehicle clears intersection
15.33	00153	1149.75	-149.75	75	Yellow	0.5	00158	00158	
15.8	00153	1185	-185	75	Red				

B.2.3 Call On Cross-Street at t=6

Traffic signal is resting in green on main street approach. A connected vehicle enters in DSRC range traveling at the Approach Speed. **Six seconds after entering DSRC range, the traffic signal control receives a call for service on a cross-street approach.** For ease of calculations, the CV enters DSRC range at exactly the beginning of the hour. All times are reported as timestamps from top of hour.

Vehicle enters DSRC range at exactly top of hour (t=0)

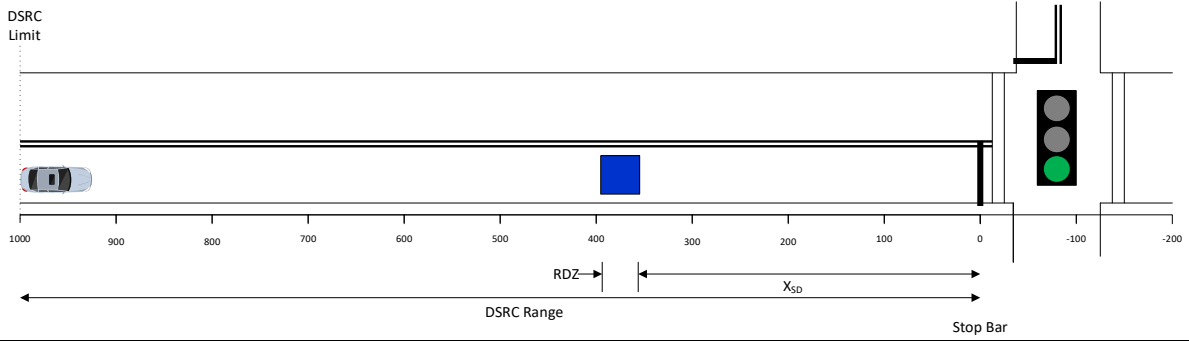
- No call on cross street



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00000	0	1000	75	Green	-	00001	36111

t=1 seconds after vehicle enters DSRC range

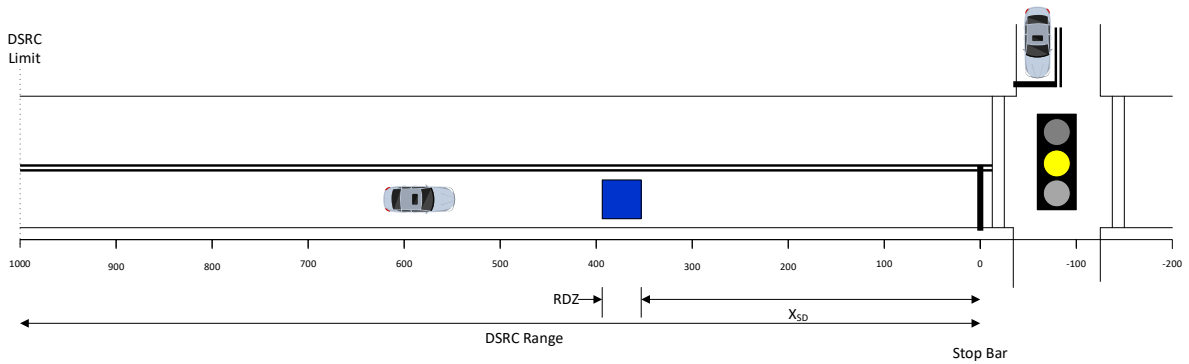
- Vehicle has traveled 75 ft. since entering DSRC range
- No call on cross street



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00010	75	925	75	Green	-	00011	36111

t=6 seconds after vehicle enters DSRC range

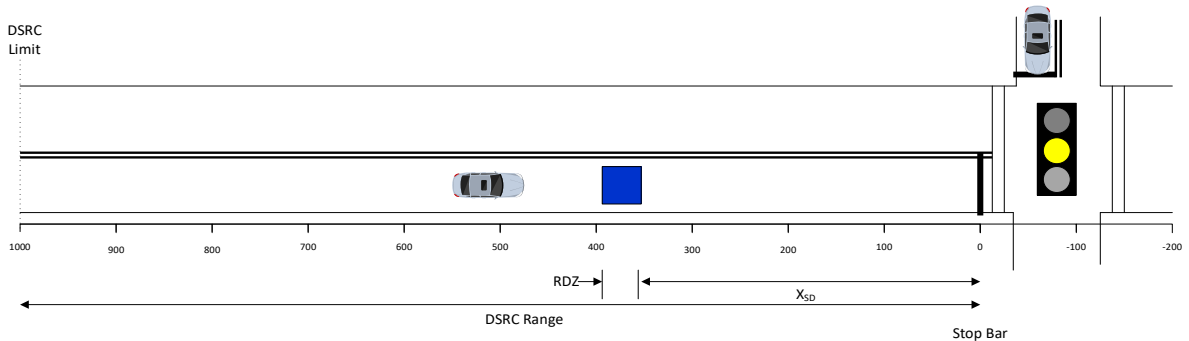
- Controller registers call on cross street
- CV has sufficient room to stop



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00060	450	550	75	Yellow	-	00110	00110

t=7 seconds after vehicle enters DSRC range

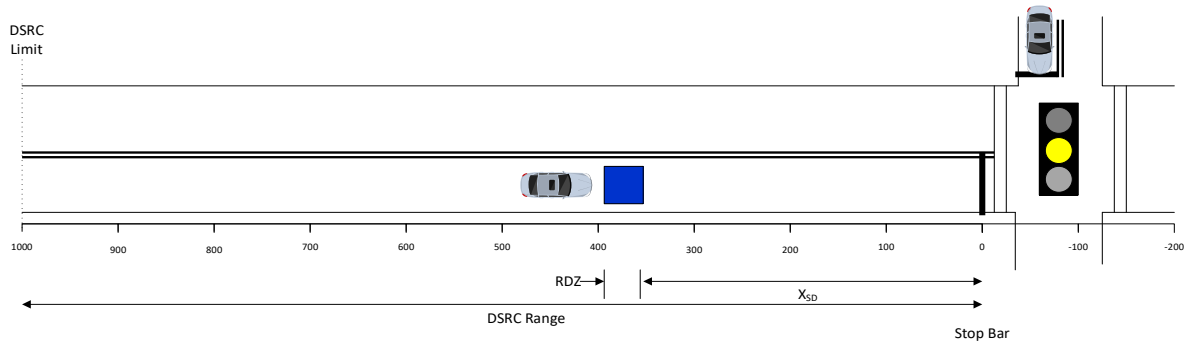
- Driver completes perception/reaction time to signal



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00070	525	475	75	Yellow	-	00110	00110

$t=8$ seconds after vehicle enters DSRC range

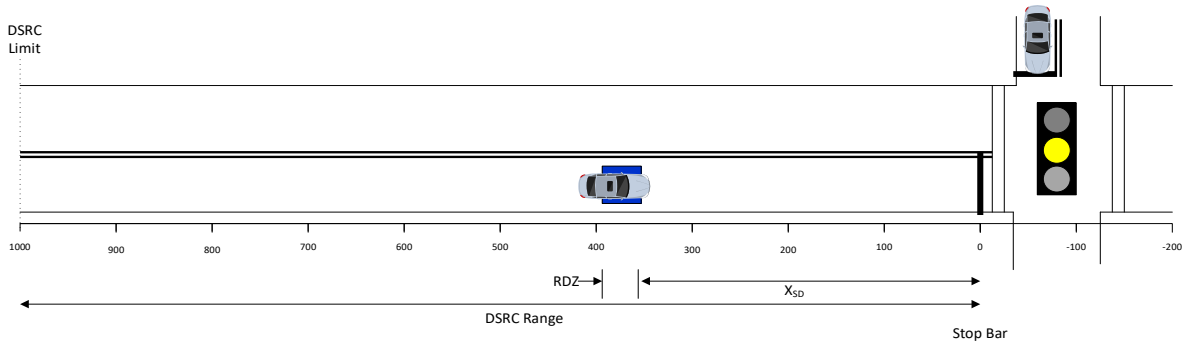
- Vehicle braking for 1 second



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00081	595	405	75	Yellow	-	00110	00110

$t=9.0$ seconds after vehicle enters DSRC range

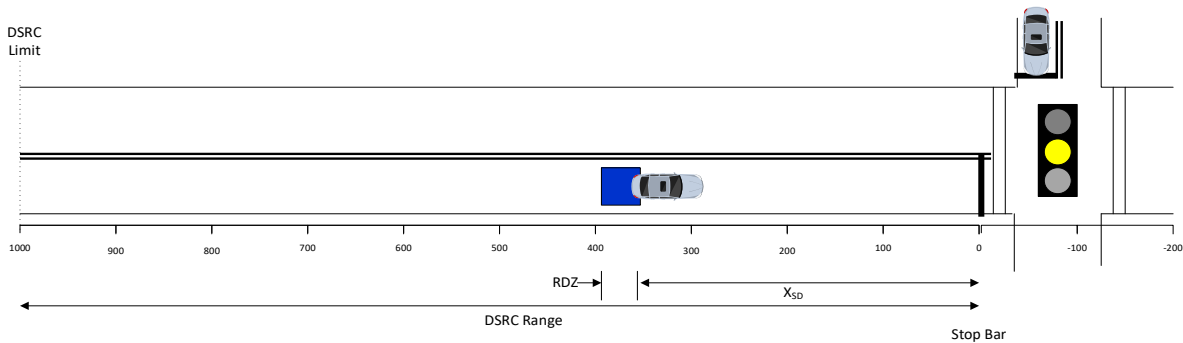
- Vehicle braking for 2 seconds



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00090	655	345	75	Yellow	-	00110	00110

$t=10.0$ seconds after vehicle enters DSRC range

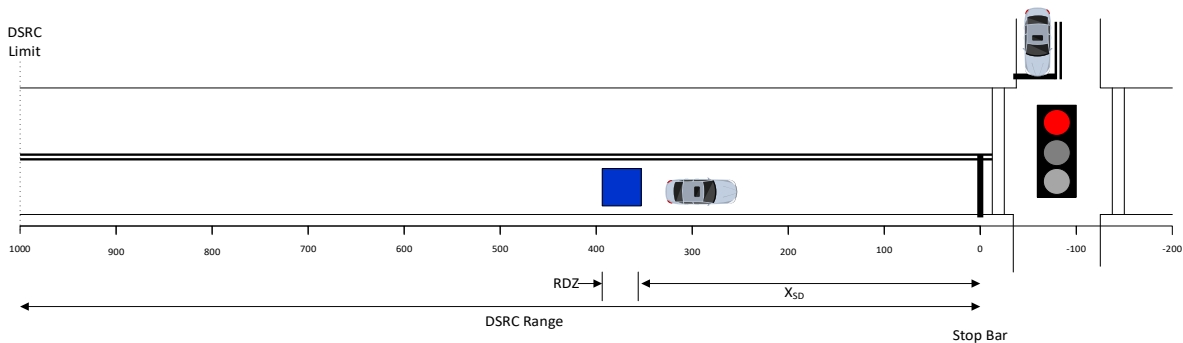
- Vehicle braking for 3 seconds



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00100	705	295	75	Yellow	-	00110	00110

$t=11.0$ seconds after vehicle enters DSRC range

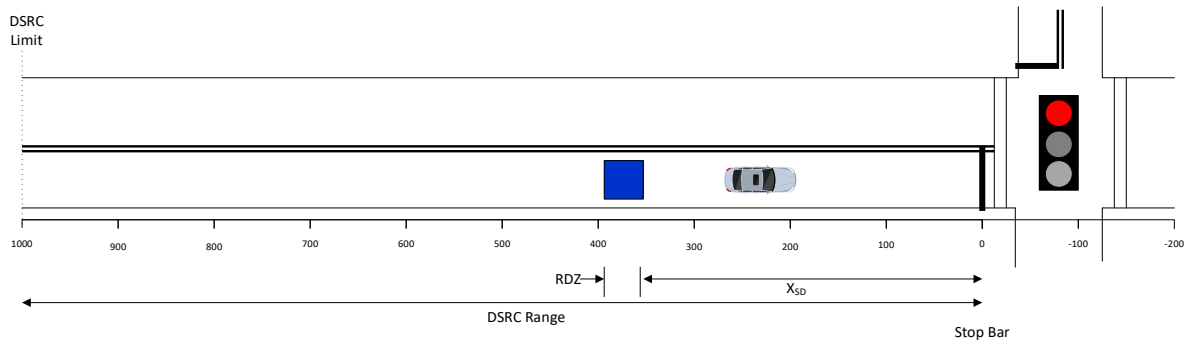
- Vehicle braking for 4 seconds
- Signal transitions to red



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00110	745	255	35	Red	-		

$t=13.5$ seconds after vehicle enters DSRC range

- Vehicle comes to stop



Timemark	Distance traveled (ft)	Distance to Stop Line (ft)	Speed of vehicle fps	Signal Status	AGP Remaining (sec)	minEndTime (timemark)	maxEndTime (timemark)
00135	805	195	0	Red	-		

Summary

Seconds from RSU Entry	Current Timemark	Distance From RSU Range	Distance to Stop Bar	Vehicle Speed (fps)	Signal Status	time to change Remaining	minEndTime	maxEndTime	
0	00000	0	1000	75	Green	0.1	00001	36111	
1	00010	75	925	75	Green	0.1	00011	36111	
6	00060	450	550	75	Yellow	5	00110	00110	Cross on Cross Street; Signal tra
7	00070	525	475	75	Yellow	4	00110	00110	Complete Perception Reaction
8	00080	595	405	65	Yellow	3	00110	00110	Decelerating for 1 sec
8.1	00081	601.45	398.55	55	Yellow	2.9	00110	00110	
8.5	00085	626.25	373.75	45	Yellow	2.5	00110	00110	
9	00090	655	345	55	Yellow	2	00110	00110	Decelerating for 2 sec
10	00010	705	295	45	Yellow	1	00110	00110	Decelerating for 3 sec
11	00110	745	255	35	Red				Decelerating for 4 sec
12	00120	775	225	15	Red				Decelerating for 5 sec
13	00130	795	205	5	Red				Decelerating for 6 sec
13.5	00135	805	195	0					Decelerating for 7 sec
									Vehicle comes to stop

Annex C Additional Information - Positioning [Informative]

C.1 RTCM Corrections (MSM4 Messages Only) Broadcast Rate Calculations

In its initial design, the rate of transmission of the GNSS correction messages was left open but for practical reasons 1 Hz was used. The experimental data showed that it took about four messages to get to a sufficient position accuracy for the vehicles for a GPS L1 receiver. This constitutes an upper bound since the rate of convergence for multi-frequency receivers is faster (need a reference for that). The required communication distance and the rate at which the correction is sent depends on the intersection approach speed and on packet error rates. The communication distance is also dependent on the fading environment for the V2X signal, which is dependent on intersection geometry, height of antenna over ground, signal power, etc. Packet error rates are dependent on the communication distance, the channel load and the packet size. This shows that determining the required transmission rate is a multidimensional problem where many parameters can be tuned. Most of the parameters are based on experienced in prior V2X projects.

The minimum needs are the following:

- L1 receiver in the vehicle with the capability of processing RTK corrections
- Correction broadcast rate is tunable up to at least 10 Hz
- Vehicle needs to position and match itself to the correct lane (where required) before it reaches the warning distance for the intersection
- The requirements for the warning distance are defined in Section 3.3.3.5.2.2, where $V_a = 85^{\text{th}}$ percentile speed OR Speed Limit + 7 mph

The vehicle should receive four correction messages to calculate the position with sufficient accuracy. As stated above, this applies for a GPS L1 receiver and could be reduced for a multi-constellation, multi-frequency receiver.

Transmission distance is dependent on output power, height of RSU antenna over ground, fading environment and line of sight distance.

For any installation, the height of the antenna over ground should be at least vehicle height so that the situation is comparable to a V2V communication environment. Ideally, the antennas should be mounted much higher, e.g., on a mast arm or the top of the pole of a traffic light to increase communication distance

Transmission power should be the maximum allowed power for the channel the messages are broadcast in.

The following calculations are based on Packet error rates of 0.1 (10%) and 0.5 (50%)

Approach speed:	V_a
Packet error rate:	PER
Warning distance:	D_{warn}
Perception Reaction time:	T_{PRT}
Deceleration:	A
Transmission Rate:	R_T
Number of required messages:	N_{Msg}
Transmission distance:	D_t

The warning distance can be calculated as the following:

$$D_{\text{warn}} = V_a^2 / (2 * A) + T_{\text{PRT}} * V_a$$

This is somewhat simplistic since it does not take into account the rise time of braking torque and assumes a constant deceleration and approach speed, but this can be subsumed into average speeds and decelerations and is for our purposes accurate enough.

Receiving four messages where the packet error rate (PER) is larger than 0 is a probabilistic process that can be modeled as a Binomial Distribution. If the probability to receive at least four messages needs to be larger than 0.9 (90%), then for PER = 0.5 and PER = 0.1 the required number of transmitted messages is:

Table 18. Required Number of RTCM Corrections Messages

Packet Error Rate	0.5	0.1
Required Number of Messages	12	5

The overall transmission distance for a uniform PER then amounts to:

$$D_t = D_{\text{warn}} + N_{\text{Msg}} / R_T * V_a$$

$$= V_a^2 / (2 * A) + (T_{\text{PRT}} + N_{\text{Msg}} / R_T) * V_a$$

For various approach speeds this distance is (for A=0.3 g and R_T = 1 Hz):

Table 19. RTCM Corrections - Warning Distances @ 1 Hz

V_a\PER (MPH)	V_a\PER (meters per second)	D_warn (meters)	D_t (PER = 0.1) (meters)	D_t (PER = 0.5) (meters)
25	11.1	37.2	92.8	170.6
30	13.3	49.6	116.3	209.6
35	15.6	63.7	141.4	250.3
40	17.8	79.3	168.2	292.7
45	20	96.7	196.7	336.7
50	22.2	115.6	226.7	382.3
55	24.4	136.3	258.5	429.6

Obviously, the PER is not constant over the length of the approach and a PER of 0.5 at a distance of more than 400 meters is reasonable (0.4), whereas at a distance of 300 meters, the PER is around 0.3 and at 125 meters it is around 0.1 for a freeway environment (*Reliability Analysis of DSRC Wireless Communication for Vehicle Safety Applications*, Fan Bai, Hariharan Krishnan, <http://citeseer.ist.psu.edu/viewdoc/download;jsessionid=56F1A030F87466E1E58670D001878A9C?doi=10.1.1.470.998&rep=rep1&type=pdf>).

The transmission distances are also achievable, even with antennas at vehicle height.

If the rate is increased to 5 Hz, assuming that the vehicle receivers refresh at the same rate, the numbers change as shown in Table 20.

Table 20. RTCMCorrections - Warning Distances @ 5 Hz

V_a\PER (MPH)	V_a\PER (meters per second)	D_warn (meters)	D_t (PER = 0.1) (meters)	D_t (PER = 0.5) (meters)
25	11.1	37.2	48.4	63.9
30	13.3	49.6	63.0	81.6
35	15.6	63.7	79.2	101.0
40	17.8	79.3	97.1	122.0
45	20	96.7	116.7	144.7
50	22.2	115.6	137.9	169.0
55	24.4	136.3	160.7	194.9

The numbers show that broadcast rates of 1 Hz work, assuming that the broadcast distance is long enough. If the broadcast distance is too short due to obstacles or challenging fading environment, then the transmission rate for the corrections needs to be increased.

The requirements could be formulated as follows:

- The intersection shall broadcast the GNSS corrections at a rate that enables the vehicle to receive at least four messages before reaching the warning distance for the 85th percentile of the intersection approach speeds or the posted speed plus 7 mph.
- The broadcast rate of the GNSS corrections shall be adjustable up to the maximum refresh rate of the base station receiver on which the corrections are based or the service that is used. Realistically this would not exceed whatever rates in-vehicle receivers can accommodate.
- The rate at which the message is broadcast shall take into account the transmission distance at which the PER is 0.7 at low channel load and the distance at normal channel loads that are observed by the RSU (to determine the likely PER based on the length of the message; this might mean that the RSU needs to have a model of the PER for the intersection).

A simple criterion for determining the broadcast rate for the corrections is

$$\text{Distance} = \frac{V^2}{2A} + \text{PRT} * V + (N/\text{Rate}) * V$$

warn distance approach distance to receive N messages

For a PRT of 1.5 seconds, a deceleration of a= 0.3 g and sending N=6 messages to receive four within the approach, the distance amounts to:

$$\text{Distance} = V^2/6 + 1.5 * V + 6/R * V$$

If Distance is greater than transmission distance then R needs to be increased. To solve for R:

$$R > 6.5 * 25 / (\text{Distance} - V^2/2A)$$

For a speed of 25 meters/second (around 55 mph), A=3 m/sec², a transmission distance of 300 meters, R has to be greater than:

$$R > 6.5 * 25 / (300 - 25^2/6) = 0.83$$

which evidently is the case. If with the same numbers, the transmission distance would only be 150 meters, R would have to be greater than 3.5 Hz.

Annex D Security Profiles [Normative]

This Annex shows the *IEEE Std 1609.2-2016* security profiles and related material for the various V2X messages sent from the RSU to the OBUs: SPaT, MAP, and RTCM corrections.

D.1 Security Profile for SPaT Messages

The following topics are addressed herein:

- Identification of application message constraints and usage of application-sensitive *SAE J2735_202007* SPaT message fields
- *IEEE Std 1609.2-2016* certificate Service Specific Permissions (SSP) required to permit sensitive application activities
- *IEEE Std 1609.2-2016* security profile for message sending, receiving and security management

Definitions included herein are meant for both V2X application specifiers as well as deployers of the technology.

D.1.1 Summary

A security summary of the application is provided in the following table.

Table 21. SPaT Application Security Summary

V2I Application / Message	SPaT
PSID	0x82
Certificate Type	<i>IEEE Std 1609.2-2016</i> Application Certificate
Message Signer	RSU
Message Sender	RSU
Message Receiver	OBU
Entity Activities Requiring Authorization	One entity-activity requiring SSP-based authorization within this application message is: <ul style="list-style-type: none"> – Communicate speed advisories (if they are regulatory-authorized)

D.1.2 SPaT PDU Field Use and Convention

This section imposes additional rules, definitions, and constraints on the SPaT message PDU defined in *SAE J2735_202007*.

Communication of Advisory Speeds in the PDU

The SPaT message allows for communication of intersection state information, with an option for advisory speeds in the field *SPaT.intersections.states.state-time-speeds.speeds*

If advisory speed information is included via inclusion of the field *SPaT.intersections.states.state-time-speeds.speeds*, then there is an assumption that the RSU able to provide static or dynamic advisory speeds based on intersection sensor inputs and/or configuration.

Inclusion of a speed advisory implies the IOO is allowed and able to provide speed advisories and that intersection sensors, RSU and traffic signal controller have been carefully installed, configured, and tested prior to being used convey the intersection state information. Advice for speeds too high can

negatively impact safety; too low can impede efficient mobility. Additionally, a compromised or stolen RSU can cause greater impact if it is allowed to convey speed advisories than if it is not.

D.1.3 Security Specific Permissions [Normative]

This section defines the Service Specific Permissions (SSP) for the SPaT application.

SSP Format

This section provides the Service Specific Permissions (SSP) format for the SPaT application.

SSP type: *IEEE Std 1609.2-2016* BitmapSsp

SSP length: 2-Octets

Bit Order: Most Significant Bit (MSB) is transmitted first

Encoding: Canonical Octet Encoding Rules (COER)

The following Table indicates the SPaT SSP octet scheme.

Table 22. SPaT SSP Octet Scheme

Octet(s)	Definition
0	Binary 0 (0000 0000): This version – temporary use Binary 1..255: SSP Version
1	See Table 30
6-30	Reserved for future use. Absent in current use.

The following table indicates the SSP authorizations for the SPaT application message:

Table 23. SPaT Service-Specific Permissions

Octet	Bit	Application Activity Authorizations	Value
1	0	<i>SPaT.intersections.states.speeds</i> has one or more entries for speed advisories from a regulatory source.	0: Certificate may not sign 1: Certificate may sign
1	1-7	Reserved	0

SSP Usage

This section provides conventions for utilizing the SPaT application message.

Sending SPaT messages

The SPaT message sender shall sign the PDU with a *IEEE Std 1609.2-2016* certificate indicating the signer is authorized to send a SPaT PDU, i.e., certificate contains the SPaT PSID and its certificate SSP Octet 0, Bit 7 indicates '0' (version 0, the version of this temporary SSP).

If the SPaT PDU also includes any advisory speed information for the intersection state, the signing certificate's SSP Octet 1, Bit 0 shall also indicate a '1.'

Validating SPaT messages

Upon receiving the SPaT message, the message receiver [OBU] will first evaluate if sender was authorized to send the SPaT message. This is performed by checking that the signing certificate contains a SPaT PSID and a SSP version of '0' (this version of the SSP).

If advisory speed is included, the message receiver shall also validate the SSP Octet 1, Bit 0 is set to '1..

D.1.4 IEEE Std 1609.2 Security Profile Identification [Normative]

The following table provides the identification features for the SPaT application security profile.

Table 24. SPaT Application Security Profile Identification

Name	Type	Recommended Values	Description
<i>Security Profile Version</i>	Text string	"IEEE Std 1609.2a-2017"	Indicates the version of the security profile. Shall be "IEEE Std 1609.2a-2017" for this version of the security profile.
<i>Name</i>	Text string	"SPaT Security Profile_SAE_V0"	The name to be used to refer to the profile. This should be unique among names used by security profiles that reference a particular PSID.
<i>PSIDs</i>	List of PSIDs	0x82 (uncompressed)	The PSIDs to be used by SDEEs that use this profile.
<i>Other considerations</i>	Text string	This SPaT security profile is for the ITE Connected Intersections. It is based on the one for the Connected Vehicle Pilot Program	A description of the conditions under which this security profile is to be used.

D.1.5 Sending

The following table provides the security profile for message sending within the SPaT PSID:

Table 25. SPaT Application Security Profile for Sending Messages

Name	Type	Recommended Values	Notes
<i>Sign Data</i>	enumerated	True	Sign all SPaT messages for data origin authentication and non-repudiation.
<i>Signed Data in Payload</i>	Boolean	True	
<i>External Data</i>	Boolean	False	
<i>External Data Source</i>	Text	N/A	
<i>External Data Hash Algorithm</i>	enumerated	N/A	
<i>Set Generation Time in Security Headers</i>	Boolean	True	Needed to determine if message lies within the validity period of the signing credential.
<i>Set Generation Location in Security Headers</i>	Boolean	True	Needed for credential and SPDU consistency checks.
<i>Set Expiry Time in Security Headers</i>	Boolean	False	
<i>Signed SPDU Lifetime</i>	Time interval	N/A	Short-lived messages, no lifetime.
<i>Signer Identifier Policy - Type</i>	Enumerated	Simple	
<i>Simple Signer Identifier - Policy: Minimum Inter - Cert Time</i>	Time interval (for example, "one second")	1 second	Comment: Default setting from IEEE Std 1609.2 SDEE Specifiers guidance seems reasonable. Also, SPaT is typically sent out at 10Hz so at least every 5 messages would get the cert vs. the cert hash as the signer identifier.
<i>Simple Signer Identifier Policy: Exceptions</i>	Boolean	False	
<i>Simple Signer Identifier Policy: Signer Identifier Cert Chain Length</i>	Integer or enumerated	1	Will use the RSUs EE certificate only within the message. We will assume full pre-distribution of CA certs to the vehicles.
<i>Text Signer Identifier Policy</i>	Text	N/A	
<i>Sign With Fast Verification</i>	enumerated	Compressed	
<i>EC Point Format</i>	Enumerated	Compressed	
<i>p2pcd_useInteractive-Form</i>	Boolean	N/A	
<i>p2pcd_max-ResponseBackoff</i>	Time or n/a	N/A	

Name	Type	Recommended Values	Notes
<i>p2pcd_response-ActiveTimeout</i>	Time or n/a	N/A	
<i>p2pcd_request-ActiveTimeout</i>	Time or n/a	N/A	
<i>p2pcd_observed-RequestTimeout</i>	Time or n/a	N/A	
<i>p2pcd_currentlyUsed-TriggerCertificateTime</i>	Time or n/a	N/A	
<i>p2pcd_response-CountThreshold</i>	Integer or n/a	N/A	
<i>Repeat Signed SPDUs</i>	Boolean	False	Each SPaT PDU transmitted must be uniquely signed.
<i>Time Between Signing</i>	Time or n/a	N/A	
<i>Encrypt Data</i>	enumerated	No	SPaT messages are in plaintext.

D.1.6 Receiving

The following table provides the message reception security features for the SPaT application security profile.

Table 26. SPaT Application Security Profile for Receiving Messages

Name	Type	Value	Notes
<i>Use Preprocessing</i>	Enumerated	True	The full cert chain will not be sent with SPaT messages.
<i>Verify Data</i>	Enumerated	True	Verify all SPaT messages when first received from a newly-encountered RSE and when acting based on the data within the SPaT message.
<i>Relevance: Replay</i>	Boolean	False	SPaT PDUs have generation time within them, so application behavior to detect replay is needed. Delayed SPaT messages need to be detected by the application.
<i>Relevance: Generation Time in Past</i>	Boolean	True	
<i>Validity Period</i>	Time interval	1 Minute	Within a 1-minute period, the application logic handles message latency issues. Beyond that, the security services will discard.
<i>Relevance: Generation Time in Future</i>	Boolean	True	
<i>Acceptable Future Data Period</i>	Time	30s	
<i>Generation Time Source</i>	Enumerated	Security Header	
<i>Relevance: Expiry Time</i>	Boolean	False	
<i>Expiry Time Source</i>	Enumerated	N/A	
<i>Consistency: Generation Location</i>	Boolean	True	Generation Location is required to be within the validity region of the certificate.
<i>Relevance: Generation Location Distance</i>	Boolean or "Text"	True	
<i>Validity Distance</i>	Distance in meters or "Variable"	1000m (Default)	By default, security services will reject if more than 1000m.
<i>Generation Location Source</i>	Enumerated	Security Header	
<i>Additional Geographic Consistency Conditions</i>			None
<i>Overdue CRL Tolerance</i>	Time period or text	30 days	
<i>Relevance: Certificate Expiry</i>	Boolean	True	.

Name	Type	Value	Notes
<i>Accept Encrypted Data</i>	Enumerated or text	No	This entire message should be in plaintext.

D.1.7 Security Management

The following table provides the security management features for the SPaT application security profile.

Table 27. SPaT Application Security Management Security Profile

Name	Type	Value	Notes
<i>Signing Key Algorithm</i>	Enumerated	ecdsaNistP256withSha256	
<i>Encryption Algorithm</i>	Enumerated	N/A	
<i>Implicit or Explicit Certificates</i>	Enumerated	Implicit	
<i>EC Point Format</i>	Enumerated	Compressed	Point compression more vital on rapidly-transmitted messages.
<i>Supported Geographic Regions</i>	Array of enumerated	Rectangular, Polygon, Identified: Country and Subregions	The type of geographic region supported for conformant certificates. For example, a region could be the USA, and a subregion could be state or county. For smaller or more complex subregions, polygons or rectangles can be used.
<i>Maximum Certificate Chain Length</i>	Integer	8	
<i>Use Individual Linkage ID</i>	Boolean	N/A	
<i>Use Group Linkage ID</i>	Boolean	N/A	
<i>Signature Algorithms in Chain or CRL</i>	Sequence of Enumerated	ecdsaNistP256withSha256	

D.2 Security Profile for MAP Messages

The following topics are addressed herein:

- Identification of application message constraints and usage of application-sensitive SAE J2735_202007 MAP message fields
- IEEE Std 1609.2-2016 certificate Service Specific Permissions (SSP) required to permit sensitive application activities
- IEEE Std 1609.2-2016 security profile for message sending, receiving and security management

Definitions included herein are meant for both V2X application specifiers as well as deployers of the technology.

D.2.1 Summary

A security summary of the application is provided in the following table.

Table 28. MAP Application Security Summary

V2I Application / Message	MAP
PSID	0x20-40-97
Certificate Type	IEEE Std 1609.2 Application Certificate
Message Signer	Central traffic management application
Message Sender	RSU
Message Receiver	OBU

Entity Activities Requiring Authorization	One entity-activity requiring authorization within this application is: <ul style="list-style-type: none"> – Communicate Regulatory Speed Limits for either intersection or road segments
--	--

D.2.2 MAP PDU Field Use and Convention

This section imposes additional rules, definitions, and constraints on the MAP message PDU defined in SAE J2735_202007.

Communication of Regulatory Speed in the PDU

The MAP message allows for the following two different topology types in which regulatory speed may be communicated:

- One for intersections: MAP.intersections.[IntersectionGeometry].speedLimits
- One for road segments: MAP.roadSegments.[RoadSegment].speedLimits

Population of either of these fields with a type of regulatory speed implies an authorized regulatory agency has performed analysis to provide a static or adaptive speed limit appropriate for the intersection or roadway geometry. Thus, the authorization needed is the 'right to communicate a regulator's authorized speed.'

The following table provides the identification features for the MAP application security profile.

D.2.3 Security Specific Permissions [Normative]

SSP Format

This section provides the Service Specific Permissions (SSP) format for the MAP application.

SSP type: IEEE Std 1609.2-2016 BitmapSsp

SSP length: 2-Octets

Bit Order: Most Significant Bit (MSB) is transmitted first

Encoding: Canonical Octet Encoding Rules (COER)

The following table indicates the MAP SSP octet scheme:

Table 29. MAP SSP Octet Scheme

Octet(s)	Definition
0	SSP Version Information Binary 0 (0000 0000): This version (0), a temporary use SSP Binary 1..255: SSP Version
1	See Table 30
2-30	Reserved for future use. Absent in current use.

Table 30 indicates the SSP roles and authorizations for the MAP application message.

Table 30. MAP Service-Specific Permissions

Octet	Bit	Application Activity Authorizations	Value
1	0	MAP.roadSegments.[RoadSegment].speedLimits or MAP.intersections.[IntersectionGeometry].speedLimits has an entry Message sender authorized to indicate regulatory speed.	0: Certificate may not sign 1: Certificate may sign
1	1-7	Reserved	0

SSP Usage

This section provides conventions for utilizing the MAP application message.

Sending MAP messages

The sending of a MAP message could involve indicating a regulatory speed for a road segment or intersection.

If the sender of the MAP message provides an entry in the *MAP.roadSegments.[RoadSegment].speedLimits* or *MAP.intersections.[IntersectionGeometry].speedLimits* fields, the sender shall sign the PDU with a certificate containing an SSP indicating it has authority to sign a MAP message with one or more regulatory speeds. This SSP shall contain:

- Octet 0: 0000 0000 (This version = 0)
- Octet 1, Bit 0 is set to '1' [certificate may sign]

Validating MAP Messages

Upon receiving the MAP message, the message receiver [OBU] will first evaluate if sender was authorized to send the MAP message. This is performed by checking that the signing certificate contains the MAP PSID and a valid SSP version.

If regulatory speed information is included, the message receiver shall validate the following:

- the SSP Octet 1, Bit 0 is set to '1' for [certificate may sign MAP message with regulatory speed]

D.2.4 IEEE Std 1609.2 Security Profile Identification (Normative)

The following table provides the security profile identification features for MAP messages signed by authorized central traffic management systems and broadcast by RSUs.

Table 31. MAP Broadcast Application Security Profile Identification

Name	Type	Recommended values	Description
<i>Security Profile Version</i>	Text string	"IEEE Std 1609.2a-2017"	Indicates the version of the security profile. Shall be "IEEE Std 1609.2a-2017" for this version of the security profile.
<i>Name</i>	Text string	"MAP_Security_Profile_SAE_V0"	The name to be used to refer to the profile. This should be unique among names used by security profiles that reference a particular PSID.
<i>PSIDs</i>	List of PSIDs	0x20-40-97	The PSIDs to be used by SDEEs that use this profile.
<i>Other considerations</i>	Text string	This MAP security profile is for the ITE Connected Intersections. It is based on the one for the Connected Vehicle Pilot Program.	A description of the conditions under which this security profile is to be used.

D.2.5 Sending

The following table provides the security profile for message sending within the MAP PSID:

Table 32. MAP Application Security Profile for Sending Messages

Name	Type	Recommended Values	Notes
<i>Sign Data</i>	enumerated	True	Sign all MAP messages for data origin authentication and non-repudiation.
<i>Signed Data in Payload</i>	Boolean	True	
<i>External Data</i>	Boolean	False	
<i>External Data Source</i>	Text	N/A	
<i>External Data Hash Algorithm</i>	enumerated	N/A	
<i>Set Generation Time in Security Headers</i>	Boolean	True	
<i>Set Generation Location in Security Headers</i>	Boolean	False	Signed messages do not need to indicate generation location. The signing certificate will indicate 'authority to sign' for a given region.
<i>Set Expiry Time in Security Headers</i>	Boolean	True	Lane closures or other intersection impediments may be somewhat dynamic, requiring multiple MAP message updates within the signer authorization certificate's validity period.
<i>Signed SPDU Lifetime</i>	Time interval	Variable (Default "72 Hours")	The signing application needs to set the time interval for this SPDU lifetime. 72 hours is the default lifetime of the MAP message, however application deployers may use shorter or longer lifetimes depending on the needs and constraints of managing the infrastructure.
<i>Signer Identifier Policy Type</i>	Enumerated	Simple	
<i>Simple Signer Identifier Policy: Minimum Inter Cert Time</i>	Time interval (for example, "one second")	Always	All MAP messages will contain the signing public key certificate.
<i>Simple Signer Identifier Policy: Exceptions</i>	Boolean	False	
<i>Simple Signer Identifier Policy: Signer Identifier Cert - Chain Length</i>	Integer or enumerated	1	Will use the signer's authorization certificate only within the message. We will assume full pre-distribution of CA certs to the OBU/MUs.
<i>Text Signer Identifier Policy</i>	Text	N/A	
<i>Sign With Fast Verification</i>	enumerated	Compressed	
<i>EC Point Format</i>	Enumerated	Compressed	
<i>p2pcd_useInteractive-Form</i>	Boolean	False	
<i>p2pcd_max-ResponseBackoff</i>	Time or n/a	N/A	
<i>p2pcd_response-ActiveTimeout</i>	Time or n/a	N/A	
<i>p2pcd_request-ActiveTimeout</i>	Time or n/a	N/A	
<i>p2pcd_observed-RequestTimeout</i>	Time or n/a	N/A	
<i>p2pcd_currentlyUsed-TriggerCertificate-Time</i>	Time or n/a	N/A	
<i>p2pcd_response-CountThreshold</i>	Integer or n/a	N/A	

Name	Type	Recommended Values	Notes
<i>Repeat Signed SPDUs</i>	Boolean	True	Following the initial, transmitted MAP PDU, each following one may be a re-transmit of the first so long as they are within the validity period of the message (as set by the signing application). Note: If this is used, then message lifetime may need to be shortened to reduce the footprint of replay attacks.
<i>Time Between Signing</i>	Time or n/a	Set to Message lifetime	
<i>Encrypt Data</i>	enumerated	No	MAP messages are in plaintext.

D.2.6 Receiving

The following table provides the message reception security features for the MAP application security profile.

Table 33. MAP Application Security Profile for Receiving Messages

Name	Type	Value	Notes
<i>Use Preprocessing</i>	Enumerated	True	The full cert chain will not be sent with MAP messages.
<i>Verify Data</i>	Enumerated	True	Verify all MAP messages.
<i>Relevance: Replay</i>	Boolean	False	
<i>Relevance: Generation Time in Past</i>	Boolean	False	Security services will not perform this check. The application should discard messages that are too old.
<i>Validity Period</i>	Time interval	N/A	
<i>Relevance: Generation Time in Future</i>	Boolean	True	This allows an RSU or TMS to set future expectations for a given intersection (e.g., a planned lane closure) even if the message doesn't reflect the current intersection state.
<i>Acceptable Future Data Period</i>	Time	30 seconds	
<i>Generation Time Source</i>	Enumerated	Security Header	
<i>Relevance: Expiry Time</i>	Boolean	True	
<i>Expiry Time Source</i>	Enumerated	Security Header	
<i>Consistency: Generation Location</i>	Boolean	False	
<i>Relevance: Generation Location Distance</i>	Boolean or "Text"	False	
<i>Validity Distance</i>	Distance in meters or "Variable"	N/A	
<i>Generation Location Source</i>	Enumerated	N/A	
<i>Additional Geographic Consistency Conditions</i>			Entire area described by MAP message is required to be within the validity region of the certificate.
<i>Overdue CRL Tolerance</i>	Time period or text	30 days	
<i>Relevance: Certificate Expiry</i>	Boolean	True	
<i>Accept Encrypted Data</i>	Enumerated or text	No	This entire message should be in plaintext.

D.2.7 Security Management

The following table provides the security management features for the MAP application security profile.

Table 34. MAP Application Security Management Security Profile

Name	Type	Value	Notes
<i>Signing Key Algorithm</i>	Enumerated	ecdsaNistP256withSha256	
<i>Encryption Algorithm</i>	Enumerated	N/A	
<i>Implicit or Explicit Certificates</i>	Enumerated	Implicit	
<i>EC Point Format</i>	Enumerated	Compressed	Point compression more vital on rapidly transmitted messages.
<i>Supported Geographic Regions</i>	Array of enumerated	Rectangular, Polygon, Identified: Country and Subregions	The type of geographic region supported for conformant certificates. For example, a region could be the USA, and a subregion could be state or county. For smaller or more complex subregions, polygons or rectangles can be used.
<i>Maximum Certificate Chain Length</i>	Integer	8	
<i>Use Individual Linkage ID</i>	Boolean	N/A	
<i>Use Group Linkage ID</i>	Boolean	N/A	
<i>Signature Algorithms in Chain or CRL</i>	Sequence of Enumerated	ecdsaNistP256withSha256	

D.3 Security Profile for RTCM corrections

The following topics are addressed herein:

- Identification of application message constraints and usage of application-sensitive SAE J2735_202007 RTCM message fields
- IEEE Std 1609.2-2016 certification issuance guidance
- IEEE Std 1609.2-2016 certificate Service Specific Permissions (SSP) required to permit sensitive application activities
- IEEE Std 1609.2-2016 security profile for message sending, receiving and security management

Definitions included herein are meant for both V2X application specifiers as well as deployers of the technology.

D.3.1 Summary

A security summary of the application is provided in the following table:

Table 35. Signal status RTCM Application Security Summary

V2I Application / Message	RTCM
PSID	0x80 (RTCM Uncompressed)
Certificate Type	IEEE Std 1609.2-2016 Application Certificate
Message Signer	Traffic Management Center or RSU
Message Sender	RSU device
Message Receiver	OBU
Application Activities Requiring Authorization	A single application activity is identified with this application: <ul style="list-style-type: none"> • Indicate uncompressed RTCM GPS corrections

D.3.2 RTCM PDU Field Use and Convention

This section imposes additional rules, definitions and constraints on the RTCM message PDU defined in *SAE J2735_202007*.

D.3.3 Uncompressed GPS Correction Information

The RTCM message indicates uncompressed GPS correction information by populating the field *RTCMcorrections.msgs* with at least one entry.

D.3.4 Certificate Issuance Guidance

This section outlines guidance or rules for the validity region of RTCM signing certificates for TMCs (or other central servers) or RSUs. It assumes a stricter security posture of the backend servers compared to CI field devices like RSUs.

Guidance for setting the validity region in certificates [Informative]

- a) The validity region in an RSU RTCM certificate should be configurable but relatively small (e.g., 1-5 miles).
- b) The validity region in a TMC RTCM certificate may be large but it should include all relevant RTCM anchor points.
- c) It is expected that the SCMS policy requires that stricter device security requirements are met for devices with larger validity region in the RTCM certificate.

Rules for meaning of validity region in certificates [Normative]

- a) The RTCM certificate validity region constrains the sender to be allowed to sign only RTCM messages whose payload contains RTCM anchor point position(s) that are contained within that validity region.

D.3.5 Security Specific Permissions [Normative]

This section defines the Service Specific Permissions (SSP) for the uncompressed RTCM application.

SSP Format

This section provides the Service Specific Permissions (SSP) format for the uncompressed RTCM application.

SSP type: IEEE Std 1609.2 BitmapSsp

SSP length: 2-Octets

Bit Order: Most Significant Bit (MSB) is transmitted first

Encoding: Canonical Octet Encoding Rules (COER)

Table 29 following table indicates the RTCM SSP octet scheme.

Table 36. RTCM SSP Octet Scheme

Octet(s)	Definition
0	Binary 0 (0000 0000): This version. For temporary use only. Binary 1..255: SSP Version Note: SSP Version '0' is current
1	Reserved

SSP Usage

This section provides conventions for utilizing the signal status RTCM message SSP.

Sending the RTCM Message

The sender generates an Uncompressed RTCM PDU per *SAE J2735_202007*.

The sender's signing certificate shall contain a PSID indicating 0x80.

The sender's signing certificate SSP shall indicate it is permitted to send the RTCM message by indicating a SSP version '0' [Octet 0, Bit 0 = 0] (this version).

Geographic Constraints

The sender is allowed to sign RTCM messages that contain in the payload an RTCM source location (the anchorPoint FullPositionVector) that is contained within the validity region of the sender's certificate.

Example Usage [Non-Normative]

None

D.3.6 IEEE Std 1609.2 Security Profile Identification

The following table provides the identification features for the RTCM application security profile.

Table 37. RTCM Application Security Profile Identification

Name	Type	Recommended values	Description
<i>Security Profile Version</i>	Text string	"IEEE Std 1609.2a-2017"	Indicates the version of the security profile. Shall be "IEEE Std 1609.2a-2017" for this version of the security profile.
<i>Name</i>	Text string	"RTCM_Uncompressed-Security_Profile_SAE_V0"	The name to be used to refer to the profile. This should be unique among names used by security profiles that reference a particular PSID.
<i>PSIDs</i>	List of PSIDs	0x80	The PSIDs to be used by SDEEs that use this profile.
<i>Other considerations</i>	Text string	This RTCM security profile is for the ITE Connected Intersections.	A description of the conditions under which this security profile is to be used.

D.3.7 Sending

The following table provides the security profile for message sending within the RTCM PSID.

Table 38. RTCM Application Security Profile for Sending Messages

Name	Type	Recommended values	Notes
<i>Sign Data</i>	enumerated	True	Sign all RTCM messages for data origin authentication and non-repudiation.
<i>Signed Data in Payload</i>	Boolean	True	Consistent with practice for other SAE J2735 message sets; also, there is no good reason not to include the signed data in the payload.
<i>External Data</i>	Boolean	False	See rationale under "Signed Data in Payload." Otherwise, we need to populate - tbsData.payload.extDataHash
<i>External Data Source</i>	Text	N/A	
<i>External Data Hash Algorithm</i>	enumerated	N/A	
<i>Set Generation Time in Security Headers</i>	Boolean	True	
<i>Set Generation Location in Security Headers</i>	Boolean	False	The location is that is relevant is that of the RTCM anchor point, and that is given in the payload.
<i>Set Expiry Time in Security Headers</i>	Boolean	True	Set this to 5 minutes to prevent an attacker being able to replay slightly-too-old messages

Name	Type	Recommended values	Notes
<i>Signed SPDU Lifetime</i>	Time interval	Configurable (default 5 minutes)	RTCM corrections will be continuous, however the IEEE Std 1609 infrastructure needs an approximate notion of freshness within which it can re-transmit already signed RTCM messages. This lifetime value should be configurable by the application deployer, however 5 minutes is a reasonable default value.
<i>Signer Identifier Policy Type</i>	Enumerated	Simple	
<i>Simple Signer Identifier Policy: Minimum Inter Cert Time</i>	Time interval (for example, "one second")	Always	All RTCM messages will contain the signing public key certificate so that a vehicle can get the benefit of RTCM even if it only receives a single message from the relevant RSU.
<i>Simple Signer Identifier Policy: Exceptions</i>	Boolean	False	No exceptions, attach cert to every signed RTCM message.
<i>Simple Signer Identifier Policy: Signer Identifier Cert - Chain Length</i>	Integer or enumerated	1	Will use the signer's authorization certificate only within the message. We will assume full pre-distribution of CA certs to the connected vehicles; this assumption is shared with the MAP and SPaT security profiles.
<i>Text Signer Identifier Policy</i>	Text	N/A	
<i>Sign With Fast Verification</i>	enumerated	Compressed	Matches convention established for other SAE J2735 messages.
<i>EC Point Format</i>	Enumerated	Compressed	Matches convention established for other SAE J2735 messages.
<i>p2pcd_useInteractive-Form</i>	Boolean	False	RTCM doesn't fit the P2PCD paradigm where the device requesting the certs sends the same messages as the device using the certs, so P2PCD doesn't work here.
<i>p2pcd_max-ResponseBackoff</i>	Time or n/a	N/A	
<i>p2pcd_response-ActiveTimeout</i>	Time or n/a	N/A	
<i>p2pcd_request-ActiveTimeout</i>	Time or n/a	N/A	
<i>p2pcd_observed-RequestTimeout</i>	Time or n/a	N/A	
<i>p2pcd_currentlyUsed-TriggerCertificate-Time</i>	Time or n/a	N/A	
<i>p2pcd_response-CountThreshold</i>	Integer or n/a	N/A	
<i>Repeat Signed SPDUs</i>	Boolean	True	While RTCM messages are dynamic, they do not change at a rate requiring each one be independently signed by the TMC. Repeats may be sent within the message lifetime.
<i>Time Between Signing</i>	Time or n/a	Set to Message lifetime	
<i>Encrypt Data</i>	enumerated	No	RTCM messages are in plaintext.

D.3.8 Receiving

The following table provides the message reception security features for the RTCM application security profile:

Table 39. RTCM Application Security Profile for Receiving Messages

Name	Type	Value	Notes
<i>Use Preprocessing</i>	Enumerated	True	The full cert chain will not be sent with RTCM messages.
<i>Verify Data</i>	Enumerated	True	Verify all RTCM messages.
<i>Relevance: Replay</i>	Boolean	False	Replayed messages are simply duplicated data, not an attack.
<i>Relevance: Generation Time in Past</i>	Boolean	False	We use expiry time, not generation time, to decide whether to reject messages.
<i>Validity Period</i>	Time interval	N/A	We use expiry time, not generation time, to decide whether to reject messages.
<i>Relevance: Generation Time in Future</i>	Boolean	True	Security services should check to make sure the message was not generated in the future
<i>Acceptable Future Data Period</i>	Time	1s	Accept 1s of skew between vehicle's clock and other devices in case of poor GPS reception by the vehicle.
<i>Generation Time Source</i>	Enumerated	Security Header	
<i>Relevance: Expiry Time</i>	Boolean	True	Require messages to expire every 5 minutes and be re-signed, to prevent an attacker from being able to replay hour-old messages and have them accepted.
<i>Expiry Time Source</i>	Enumerated	Security Header	
<i>Consistency: Generation Location</i>	Boolean	True	The consistency check is that the validity region of the TMC or RSU certificate contains the RTCM source location (the anchorPoint FullPositionVector) from the RTCM PDU payload.
<i>Relevance: Generation Location Distance</i>	Boolean or "Text"	False	
<i>Validity Distance</i>	Distance in meters or "Variable"	N/A	
<i>Generation Location Source</i>	Enumerated (headers/ payload/ other)	payload	This is the anchor PositionVector from the payload.
<i>Additional Geographic Consistency Conditions</i>	Boolean	False	
<i>Identified Region Representation Accuracy</i>	Text or N/A	N/A	
<i>Overdue CRL Tolerance</i>	Time period or text	30 days	
<i>Relevance: Certificate Expiry</i>	Boolean	True	
<i>Accept Encrypted Data</i>	Enumerated or text	No	This entire message should be in plaintext.

D.3.9 Security Management

The following table provides the security management features for the RTCM application security profile:

Table 40. RTCM Application Security Management Security Profile

Name	Type	Value	Notes
<i>Signing Key Algorithm</i>	Enumerated	ecdsaNistP256withSha256	
<i>Encryption Algorithm</i>	Enumerated	N/A	
<i>Implicit or Explicit Certificates</i>	Enumerated	Implicit	
<i>EC Point Format</i>	Enumerated	Compressed	Point compression more vital on rapidly-transmitted messages.
<i>Supported Geographic Regions</i>	Array of enumerated	Rectangular, Polygon, Identified: Country and Subregions	The type of geographic region supported for conformant certificates. For example, a region could be the US, and a subregion could be state or county. For smaller or more complex subregions, polygons or rectangles can be used.
<i>Maximum Certificate Chain Length</i>	Integer	8	
<i>Use Individual Linkage ID</i>	Boolean	N/A	
<i>Use Group Linkage ID</i>	Boolean	N/A	
<i>Signature Algorithms in Chain or CRL</i>	Sequence of Enumerated	ecdsaNistP256withSha256	

Annex E Additional Information - Security [Informative]

E.1 Securing Messages From Source to End Recipient (Example)

Let us say a communication system is such that a Message is produced by a device and is meant to be consumed by an end recipient. Message trustworthiness is paramount, and is achieved, in this scenario, by a (digital) signature that can be attached to the Message. Signatures have the benefit that if the Message or its signature is changed in any way, the recipient will be able to tell and so can discard that Message as untrustworthy. This is called “integrity protection.”

For illustration sake let us imagine a system where messages are produced and need to get delivered to a community of receivers, who can be assured of their trustworthiness. A trustworthy device Alice produces messages M. Another trustworthy device Bob gets messages from Alice, and then sends them to a community of receivers. The communication channels between Alice, Bob, and the community may or may not be trusted; i.e., the channels may harbor attackers that can alter messages. In particular, the communication between Bob and the community of receivers is not secured. The receivers trust both Alice and Bob, i.e., can verify the signatures of either Alice or Bob on a given message, and that is sufficient to establish trustworthiness of the signed message. That is, recipients trust a message M if they can be assured that:

- a) Alice produced it; and
- b) it hasn't been modified in its journey from Alice to them.

Let's look at two scenarios and go through the journey of a message M:

- a) Alice produces the message and can sign it herself.
- b) Alice produces the message but cannot sign it herself; only Bob can sign messages.

Scenario 1 is an illustration of the case of MAP messages, which get produced and signed by the MAP server and then distributed via the RSU for subsequent transmission to vehicles. Scenario 2 represents the case of SPAT messages, which get produced by the Traffic Signal controller, signed by the RSU, and then transmitted to vehicles.

We will show (informally) that a receiver can be assured a received message is trustworthy in both scenarios, with some conditions.

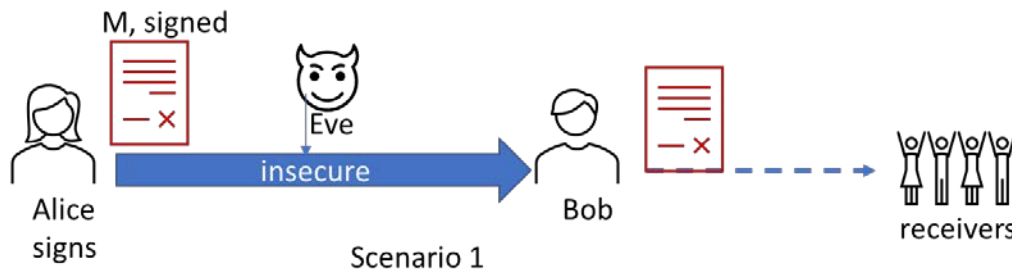


Figure 40. Security Scenario 1.

Scenario 1: Since Alice is both the producer of the message and the signer of it, once a message M is signed, it has integrity protection which allows it to travel through untrustworthy channels and be passed via Bob or other devices, and the receivers can still verify that M was indeed produced by Alice and not altered. Thus both a) and b) are easily satisfied, by virtue of digital signatures applied at the source (Alice).

But can Scenario 2 be “just as good” as Scenario 1 in terms of assurance that the receiver can have? Scenario 2 needs some expansion. Alice produces M, and since she can’t sign it, she has to send it to Bob to sign. But if another device, Eve, gets between Alice and Bob, and intercepts this message and changes it from M to M’, then Bob has no way to know: Bob will sign what he thinks Alice sent him, the changed message M’. Then after disseminating it to the community, the receivers will verify Bob’s signature and wrongly assume that the M’ they received is trustworthy.

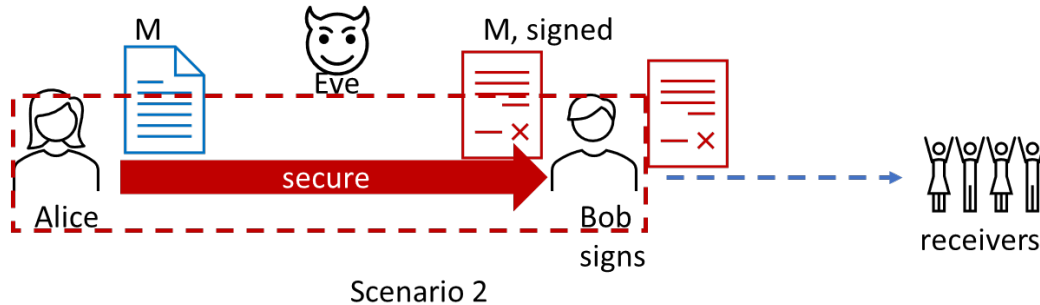


Figure 41. Security Scenario 2.

In order to prevent this from happening, the communication channel between Alice and Bob must be secure in that no other device Eve can modify messages exchanged between them and go undetected. That is, if Bob can be assured that a message M he receives is exactly what Alice meant to send him, then Bob can go ahead and sign M and distribute it to the receivers; they will verify Bob’s signature on Alice’s message, and since they trust Bob and know that the message is truly the one Alice produced, they can be assured of both a) and b): of a), because only Alice produces such content; and of b), because the message was securely transferred between Alice and Bob, and was signed by Bob, sent to them via the (insecure) communication channel.

In Scenario 2, the secure channel between Alice and Bob allows us to view Alice and Bob as a team, as a single unit around which one can draw a “security boundary.”

Our community of receivers can be assured that the messages they receive are trustworthy!

E.2 Certification Process

This section gives an overview of the Connected Intersection certification process. The elements involved are the following:

- **IOO or Operating Agency.** The IOO personnel (or process) responsible for the network security, where the network includes the Center and Field devices, and their interfaces. The IOO produces security compliance assessment documentation.
- **Point of Certification (POC).** An entity approved by the CI ecosystem, that evaluates compliance assessments from IOOs, in order to determine whether the CI network attains a certain level of security for a given set of aspects, and formalize this result in a security certification.
Note: For this version of this document, the POC is the IOO itself, and the certification is in effect a self-declaration.
- **SCMS provider.** An infrastructure-based security credential management system (SCMS) responsible for generating and delivering the *IEEE Std 1609.2-2016* security certificates that are used in the verification process of messages “between mobile elements and field infrastructure.”
- **(D)TLS certificate provider.** An infrastructure-based credential management system responsible for generating and delivering the X.509 security certificates.

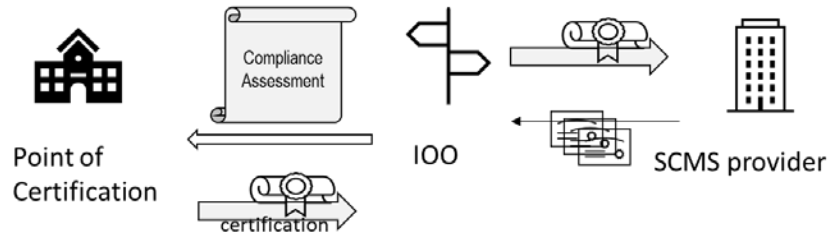


Figure 42. CI Certification Ecosystem

The CI ecosystem is involved in selecting or designating POCs. A system may have multiple POCs. The certifications that the POC produces are valid for a given amount of time (e.g., 1 year). The certification process is as follows:

1. The IOO assembles a security compliance assessment documentation. In the future, the IOO may employ third parties to perform security audits, penetration testing, or other such operations that result in attestation of the security posture of the network. This documentation is then provided to a designated POC.
2. The POC in turn evaluates the assessment and decides whether the IOO attains the security levels as expected. As a result, the POC returns to the IOO either a formal security certification or a result indicating further measures are to be employed and/or current measures adjusted. The IOO can then implement the additional measures and/or adjust the existing ones, and produce updated compliance assessment documentation.
3. Once the IOO obtains a security certification from the POC, the IOO can submit it to a SCMS provider, who then is able to issue certificates to the devices (e.g., RSUs) or servers (e.g., MAP server) in the IOO network.
4. The IOO can follow step 3 for a TLS certificate provider.

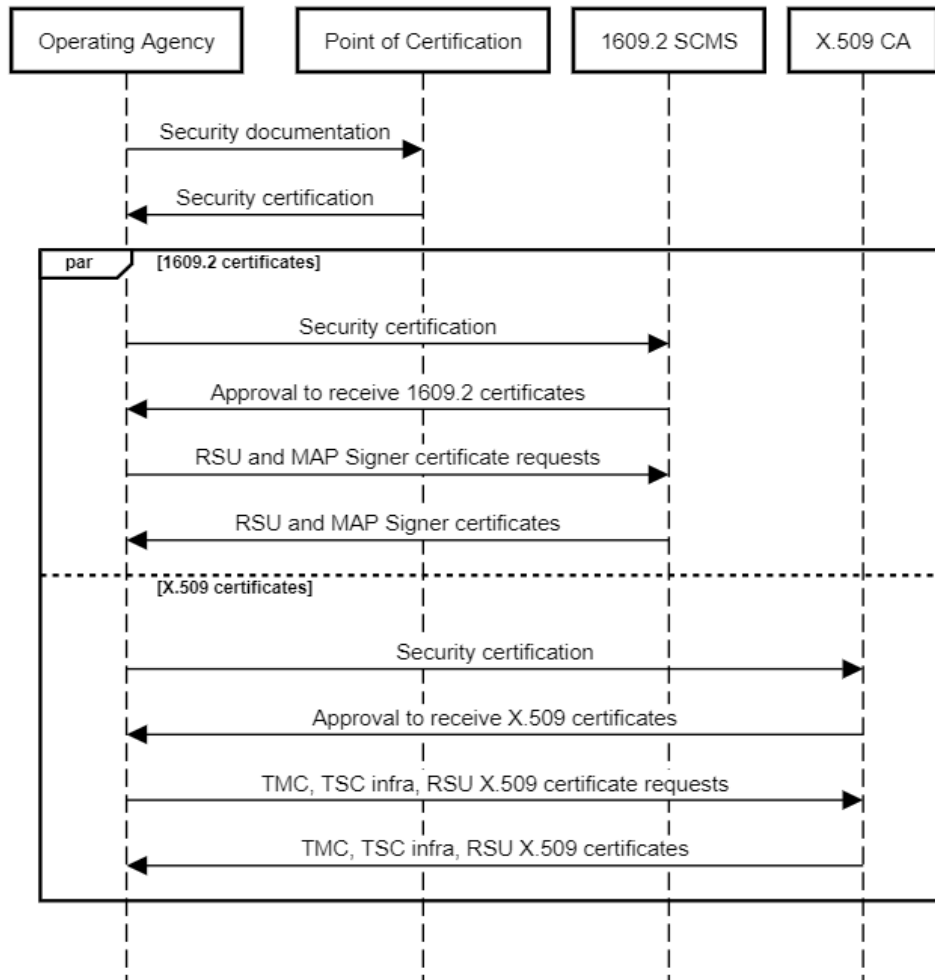


Figure 43. CI Certification Process

E.3 Attack Tree Examples

E.3.1 Introduction

Attack trees and mitigations are part of the security compliance assessment documentation that an IOO can provide in order to show the security posture of their ITS deployment. This section provides a brief introduction to attack trees.

Attack trees are one of the oldest and most widely used methods to model threats, applicable to cyber-only systems, cyber-physical systems, and purely physical systems. At first, attack trees were applied as a stand-alone method, but over the years they have been used in conjunction with and as a helper to threat frameworks-based methodologies such as Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE) and MITRE ATT&CK® (Adversarial Tactics, Techniques and Common Knowledge).

Attack trees, also known as threat trees, were first introduced in 1999, and to this day they are still used in many systems to model adversarial threats and design respective mitigations. They are a tool to help enumerate the security threats an organization may face. The path that an adversary takes is described in a hierarchical or tree format: The root of the tree constitutes the overall goal of the attack, while the branch nodes indicate methods of achieving that goal. Each branch node represents an attack (action, event, activity), which in turn is the goal for the nodes beneath it, also referred to as child attacks. In

summary, attack trees are a tool that helps with the tasks of threat brainstorming, adversary modeling, and mitigation development. An example of a simple attack tree is shown in Figure 44.

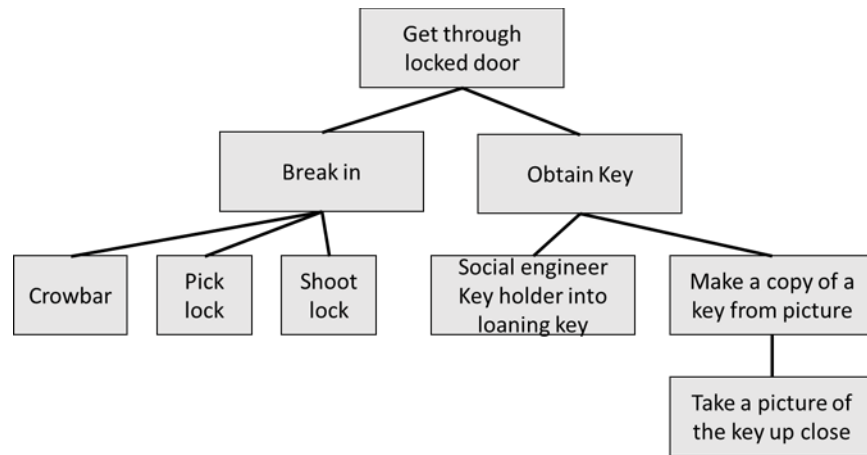


Figure 44. Example of Attack Tree.

E.3.2 Attack Tree Building Preliminaries

In the following sections, examples of attack trees will be shown for each use case (attack goal). Importantly, they are only **examples** for educational purposes; each IOO should construct their own based on their deployment. A tree diagram is also provided for illustrative purposes.

There are several attack trees that will be constructed, largely covering incorrect RSU outputs over the RSU-OBU interface. For the purposes herein, these are considered attacks, even though these events may also happen as a result of non-malicious misconfiguration or anomalous device behavior. The reason is if these misconfigurations or unintended behaviors are maliciously sourced, they may cause significant harm (e.g., to safety of vehicles using this information).

An attack tree may contain sub-trees, which are used to avoid a repetition of common attack tree segments (e.g., hacking the TMS or the MAP server require very similar steps). More basically, for each “parent” attack node in the attack tree, there are one or more actions that may or must take place in order to reach its goal, either independently (i.e., they are “disjunctive”), or necessarily together (i.e., they are “conjunctive”).

Each attack listed in the tree is to be accompanied by one or more mitigations that address that attack. Mitigations are measures that are expected to decrease the chance of an actual attack being successfully undertaken by an adversary; they are usually preemptive security controls, which are reasonable in terms of cost and continuous operation of the system. Mitigations can also be used to address the impact of a successful attack. If the risk from an attack (the combination of likelihood and impact) is believed to be sufficiently low, the mitigation can be recorded as “Attack is low risk, no mitigation required.” The rules for mitigations recording are the following:

- All attacks must have recorded a mitigation or no need for mitigation.
- If an attack has child attacks, the mitigations should be specified at the level of the child attacks (this applies recursively). For example, a parent node mitigation includes “see child attack mitigations.”
 - This ensures that the complete mitigation for each identified attack can be identified without having to read “up the tree.”
 - This may result in duplicate mitigations being recorded in the tree: the duplicate mitigations can be combined into a single instance when the material from the tree is later used to create system requirements.
- Record the parent mitigation on each child attack even at the cost of duplication.

- If an attack does not have any child attacks it must have a stand-alone mitigation recorded for it.
- On child attacks where the mitigation recorded for the parent attack *fully mitigates* the child attack too, one can record the mitigation as “See mitigation on parent”.

It is important to note that a judgement call must be made about the level of detail to include in the attack tree. Including excessive detail makes the attack tree unwieldy, while omitting detail might lead to a threat not being covered that requires a specific mitigation, resulting in that mitigation not being implemented. Good guidance is that the attack tree should go to a level where the statement of the mitigation for an attack allows the attack to be completely mitigated – in other words, if there are child attacks that require significantly different mitigations from each other, the tree should be extended to explicitly capture those child attacks.

The following attack goals are in scope (from Section 3.3.4.3.1, Security Compliance Assessment):

1. RSU outputs incorrect SPaT messages
2. RSU outputs incorrect MAP messages
3. RSU outputs incorrect positioning corrections (RTCM)

A SPaT, MAP, or RTCM message is considered “incorrect” if it fails to meet the requirements and design set forth in this document: for example, it does not match the actual traffic light signal from the TSC, does not fulfill applicable accuracy requirements, or it contains an invalid signature by the conditions of IEEE 1609.2 and its security profile.

E.3.3 Constructing an Attack Tree: RSU Outputs Incorrect SPaT Messages

An *example* attack tree showing some of the attacks that may cause an RSU to output incorrect SPaT messages is shown in Figure 45 below, and is provided for illustrative purposes only. Such figures are optional to the IOO documentation. The attack tree can be described in list format, an example of which is shown next.

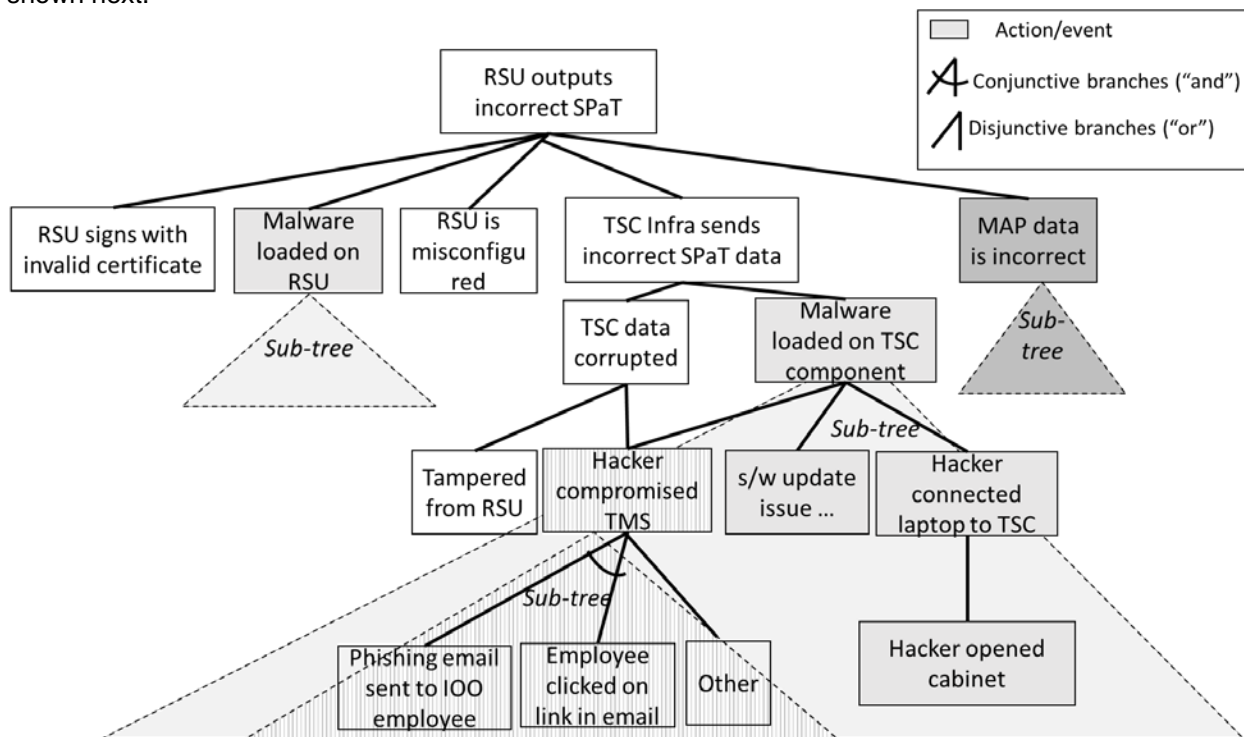


Figure 45. Attack Tree Example - RSU Outputs Incorrect SPaT Messages.

“RSU outputs incorrect SPaT messages” attack tree

1. RSU outputs incorrect SPaT messages.

Possible actions that lead to this state are any of the following:

- 1.1. RSU signs with an invalid certificate. Possible actions that lead to this state are any of the following (not shown in the diagram):
 - 1.1.1. RSU signs with an expired certificate. This may occur because the RSU's own certificate has expired or one in its chain has expired, and the RSU signing software does not check that the certificate is expired before signing.
 - 1.1.2. RSU signs with a certificate with incorrect Provider Service Identifier (PSID). This may occur because the RSU's certificate has the incorrect PSID and the RSU signing software does not check that the certificate has the correct permissions before signing.
 - 1.1.3. (Other attacks can be inserted here based on the ways in which a message can be inconsistent with the certificate as specified in IEEE 1609.2 – for example, inconsistent SSP, inconsistent geographic region, etc. Alternatively, all the attacks that are mitigated by correct implementation of IEEE1609.2, will not be enumerated.)
- 1.2. Malware loaded on RSU causes incorrect SPaT messages to be constructed by the RSU. Possible actions that lead to this state are described in the “**Malware loaded on RSU**” sub-tree.
- 1.3. RSU is misconfigured. Possible actions that lead to this state are any of the following (not shown in the diagram):
 - 1.3.1. RSU time source is caused to be out of sync. Possible actions that lead to this state are any of the following:
 - 1.3.1.1. Attacker with logical access resets the clock.
 - 1.3.1.2. Hardware error in clock chip leads to clock being out of sync with real time.
 - 1.3.2. RSU is provided with incorrect map data to use to turn TSC information into SPaT lanes.
 - 1.3.3. (other general misconfiguration actions or attacks)
- 1.4. TSC Infrastructure sends incorrect SPaT data to the RSU. Possible actions that lead to this state are:
 - 1.4.1. TSC data is corrupted. Possible actions that lead to this state are:
 - 1.4.1.1. Hacker compromised TMS. The hacker can use the TMS to spoof TSC data. Possible actions that lead to this state are described in the “**Hacker compromised TMS**” attack sub-tree.
 - 1.4.1.2. TSC data is tampered with or spoofed in transit between TSC and the RSU. Possible actions that lead to this state are: hacker compromised a middlebox (router, switch) in the ITS network and is able to alter the data without detection, due to lack of transport-layer security (TLS).
 - 1.4.2. Malware loaded on the TSC infrastructure component. Possible actions that lead to this state are described in the “**Malware loaded on TSC**” sub-tree.
- 1.5. MAP data is incorrect, so the RSU makes an incorrect translation from TSC information to SPaT format. Possible actions that lead to this state are described in the “**MAP data is incorrect**” sub-tree (next section).

“**Hacker compromised TMS**” attack subtree

Hacker (adversary) compromises TMS server. Possible actions that lead to this state are *both of the following*:

1. Phishing email is sent to IOO employee by hacker; AND
2. Employee clicks on link from email that downloads malware on the IOO internal network.

Another possible type of action is:

3. Compromise server via means other than email phishing.

“**Malware loaded on <component>**” attack subtree

Both the RSU and the TSC attack sub-trees are described here since they are very similar. Malware here is an extraneous piece of software that causes incorrect SPaT data or messages to be constructed by the component of the CI system (RSU, TSC infrastructure). Possible actions that lead to this state are *any of the following*:

1. Software update for the <component> has vulnerability that's being exploited by the malware. Alternatively, the software update itself contains the malware - which can be due to supply chain compromise, e.g., malicious party at the OEM or its suppliers purposely inserts this code. The software update can be from the OEM or from some other 3rd party supplier.
2. Adversary (hacker) compromises the Traffic Management System (TMS). Then the hacker can use the TMS to load malware onto the <component> via regular management signaling. Possible actions that lead to this state are described in the "**Hacker compromised TMS**" attack sub-tree.
3. Hacker connects her laptop to the <component> and uses this connection to load malware directly. A possible action that leads to this state is the following:
 - 3.1. Hacker has managed to open the cabinet door. This may be either because either of the following actions (not shown in diagram for simplicity):
 - 3.1.1. Hacker fraudulently obtained a key to the cabinet, or
 - 3.1.2. Hacker forced open the cabinet door.

Mitigations

Mitigations for the events/adversary activity listed above are listed in Table 41.

Table 41. Mitigations - RSU Outputs Incorrect SPaT Messages

Adversary Action Name	Possible Mitigation(s)
1.1 RSU signs with invalid certificate	<ol style="list-style-type: none"> 1. Track RSU certificate validity time and automatically renew it before it expires. 2. Ensure correct PSID appears in RSU certificates.
1.2 Malware loaded on RSU	<ol style="list-style-type: none"> 1. Employ Software checking at RSU. 2. Scan RSU software with up-to-date tools to detect vulnerabilities or malware. 3. Employ secure boot on RSU. 4. See child attacks mitigations.
1.2.1 Hacker compromised the TMS	<ol style="list-style-type: none"> 1. Employ Software checking at RSU. 2. Scan RSU software with up-to-date tools to detect vulnerabilities or malware. 3. Employ secure boot on RSU. 4. See entry 1.4.1.2.
1.2.2 Software update has vulnerability or malware	<ol style="list-style-type: none"> 1. Employ Software checking at RSU. 2. Scan RSU software with up-to-date tools to detect vulnerabilities or malware. 3. Employ secure boot on RSU. 4. Disallow remote software or firmware updates. 5. Ensure security of channel to receive updates from the OEM (e.g., OEM's signature on binary executable).
1.2.3 Hacker connected laptop to RSU	<ol style="list-style-type: none"> 1. Mount RSU very high up on pole. 2. See child attacks mitigations.
1.2.3.1 Hacker opened cabinet	<ol style="list-style-type: none"> 1. Mount RSU very high up on pole. 2. Monitor alerts at the TMS of open cabinet where RSU hardware is located. 3. (Possible recovery): Have means to immediately isolate (from network) the TSC if the opening was unauthorized. 4. (Possible detection): Use tamper evident sealing.
1.3 RSU is misconfigured	<ol style="list-style-type: none"> 1. Ensure time at the RSU matches true system time (Periodic check). 2. Ensure MAP data correctness to the RSU. 3. Periodically check configuration settings at the RSU (from the TMS).
1.4 TSC infrastructure sends incorrect data	<ol style="list-style-type: none"> 1. Ensure RSU software employs input validation. 2. See child attacks mitigations.
1.4.1 TSC data is corrupted	<ol style="list-style-type: none"> 1. Ensure RSU software employs input validation. 2. See child attacks mitigations.

Adversary Action Name	Possible Mitigation(s)
1.4.1.1 TSC data is tampered/ spoofed in transit from RSU	<ol style="list-style-type: none"> 1. Ensure RSU software employs input validation. 2. Connection is physically difficult to access. 3. Connection uses cryptographic authentication.
1.4.1.2. Hacker compromised the TMS	<p>(see Note 1)</p> <ol style="list-style-type: none"> 1. Employ state of the art Intrusion Prevention/Detection Systems (IPS/IDS) into the TMS network. 2. Employ threat-informed defenses and keep the set of threats up to date. 3. Employ firewalls with clearly set policies to reduce access to the TMS for external networks. 4. Ensure TMS is not accessible from the public Internet.
1.4.1.2.1 Phishing email to IOO employee	<p>1 - 4 above (1.4.1.2).</p> <ol style="list-style-type: none"> 5. Use email filtering tools.
1.4.1.2.2 Employee clicks on link from phishing email	<p>1 - 4 above (1.4.1.2)</p> <ol style="list-style-type: none"> 5. Train IOO employees about email security. 6. Periodically send test emails to determine effectiveness of training.
1.4.1.2.3 Compromise server via means other than email phishing	See mitigation on parent (1.4.1.2).
1.4.2 Malware loaded on the TSC infrastructure component	See entry 1.2 “Malware loaded on the RSU,” apply to TSC infrastructure component.
1.5 MAP data is incorrect	See entry 2.4 in “MAP data is incorrect” attack sub-tree (next section).

Note 1: Entry 1.4.1.2: This is a subtree that should be standalone since it's referenced elsewhere, so it does not have its parent's mitigations in it explicitly. For a complete mitigation of attack 1.4.1.2, include also mitigations of 1.4.1.

E.3.4 Constructing an Attack Tree: RSU Outputs Incorrect MAP Messages

An example attack tree showing some of the attacks that may cause an RSU to output incorrect MAP messages is shown in Figure 46 below, and is provided for illustrative purposes only. Such figures are optional to the IOO documentation. The attack tree can be described in list format, an example of which is shown next.

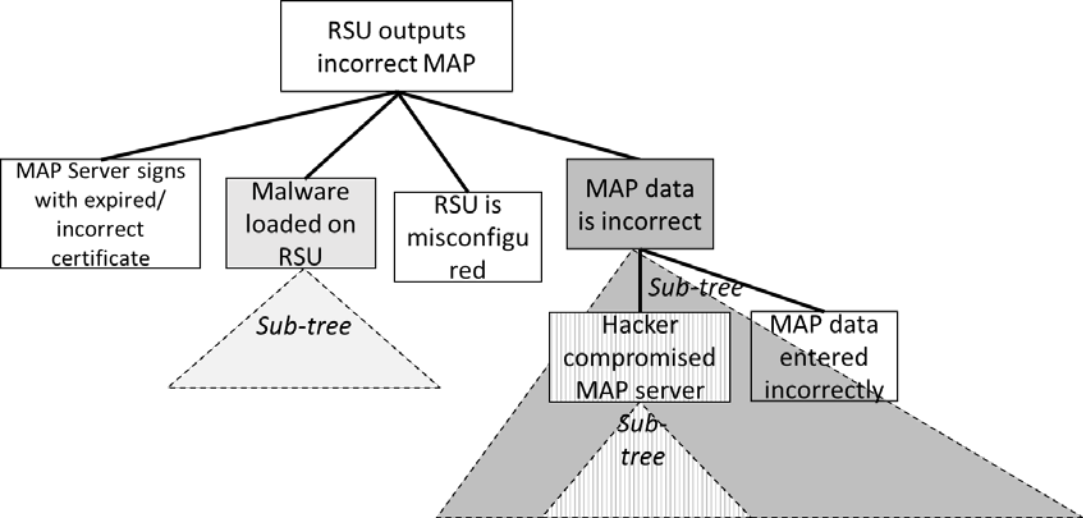


Figure 46. Attack Tree Example - RSU Outputs Incorrect MAP Messages.

“RSU outputs incorrect MAP messages” attack tree

2. RSU outputs incorrect MAP messages.

Possible actions that lead to this state are any of the following:

- 2.1. MAP server signs with invalid certificate. Possible actions that lead to this state are any of (not shown in the diagram):
 - 2.1.1. MAP server signs with expired certificate. This may occur because the MAP server's own certificate has expired or one in its chain is expired, and the MAP signing software does not check that the certificate is unexpired before signing.
 - 2.1.2. MAP server signs with certificate with incorrect Provider Service Identifier (PSID). This may occur because the MAP server's certificate has the incorrect PSID and the MAP signing software does not check that the certificate has the correct permissions before signing.
 - 2.1.3. (Other attacks can be inserted here based on the ways in which a message can be inconsistent with the certificate as specified in 1609.2 – for example, inconsistent SSP, inconsistent geographic region, ...)
- 2.2. Malware loaded on RSU causes incorrect MAP messages to be constructed by the RSU. Possible actions that lead to this state are described in the **"Malware loaded on RSU"** sub-tree.
- 2.3. RSU is misconfigured. See corresponding action (1.3) in the "RSU outputs incorrect SPaT messages" attack tree.
- 2.4. MAP data is incorrect. Possible actions that lead to this state are described in the **"MAP data is incorrect"** attack sub-tree.

"MAP data is incorrect" attack subtree

Possible actions that lead to this state are any of the following:

- 2.4.1. MAP data is tampered in transit from TMS to RSU. Possible actions that lead to this state are: Hacker compromised a middlebox (router, switch) in ITS network and is able to alter the data without detection, due to lack of transport-layer security (TLS).
- 2.4.2. Hacker compromised MAP server. Then hacker can use the MAP server to spoof MAP data that is sent. Possible actions that lead to this state are described in the **"Hacker compromised TMS"** attack sub-tree, where the "MAP Server" is substituted for the TMS.
- 2.4.3. MAP data is entered incorrectly. Possible actions that lead to this state are any of the following (not shown in the diagram):
 - 2.4.3.1. The staff who enters this data or supervises the automatic data upload accidentally enters incorrect data.
 - 2.4.3.2. Staff fails to check for correctness of input data.
 - 2.4.3.3. The data entered is not current.

Mitigations

Mitigations for the events/adversary activity listed above are listed in Table 42.

Table 42. Mitigation - RSU Outputs Incorrect MAP Messages

Adversary Action Name	Possible Mitigation(s)
2.1 MAP server signs with invalid certificate	<ol style="list-style-type: none">1. Track MAP server certificate validity time and automatically renew it before it expires.2. Ensure correct PSID appears in MAP server certificate.3. Ensure RSU checks MAP signature and does not output a MAP if it doesn't pass this check.
2.2 Malware loaded on RSU	<ol style="list-style-type: none">1. See corresponding entry 1.2 in the "RSU outputs incorrect SPaT" mitigations.
2.3 RSU is misconfigured	<ol style="list-style-type: none">1. See corresponding entry 1.3 in the "RSU outputs incorrect SPaT" mitigations.
2.4 MAP data is incorrect	<ol style="list-style-type: none">1. Ensure RSU software performs input validation for MAP data.2. See child attacks mitigations.
2.4.1 MAP data is tampered in transit from TMS to RSU	<ol style="list-style-type: none">1. Ensure RSU software performs input validation for MAP data.2. Employ TLS with integrity protection between TMS and RSU.

Adversary Action Name	Possible Mitigation(s)
2.4.2 Hacker compromised MAP server	1. Ensure RSU performs input validation for MAP data. 2. See corresponding entry 1.4.1.2 in the “RSU outputs incorrect SPaT” mitigations, with TMS being replaced by MAP server.
2.4.3 MAP data entered incorrectly	1. Attack risk is low, no mitigation.

E.3.5 Constructing an attack tree: “RSU outputs incorrect RTCM messages.”

An example attack tree showing some of the ways that may cause an RSU to output incorrect RTCM messages is similar to that of Figure 47. The difference with the MAP messages is that RTCM data can be obtained by the RSU from an online source (like a NTRIP provider), GPS receiver or cellular base station nearby, or from the TMS (for example, the TMS does its own calculation). The RSU can sign these messages or they may be already signed by the source.

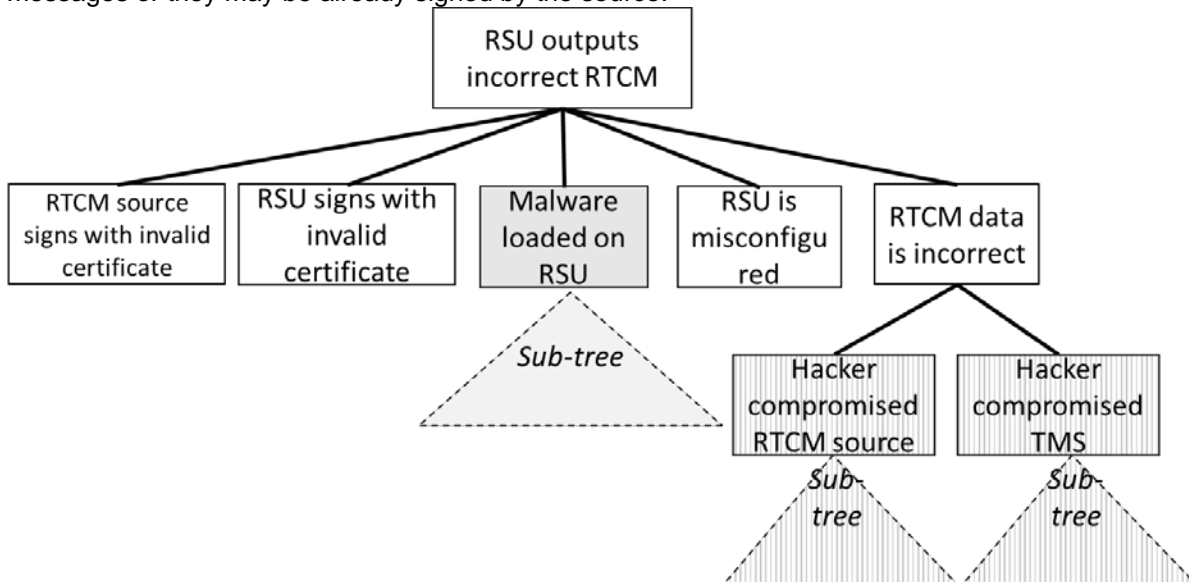


Figure 47. Attack Tree Example - RSU Outputs Incorrect RTCM Messages.

“RSU outputs incorrect RTCM messages” attack tree

3. RSU outputs incorrect RTCM messages.

Possible actions that lead to this state are any of the following:

- 3.1. RTCM source signs with invalid certificate.
- 3.2. RSU signs with invalid certificate. See the corresponding entry (1.1) in the “RSU outputs incorrect SPaT messages” attack tree.
- 3.3. Malware loaded on RSU causes incorrect RTCM messages to be constructed by the RSU. Possible actions that lead to this state are described in the “Malware loaded on RSU.”
- 3.4. RSU is misconfigured. See corresponding entry in the “RSU outputs incorrect SPaT messages” attack tree.
- 3.5. RTCM data is incorrect. Possible actions that lead to this state are any of the following:
 - 3.5.1. Hacker compromised RTCM source. Possible actions that lead to this state are described in the “Hacker compromised TMS” attack sub-tree, where the “RTCM Server” is substituted for the TMS. Another possible way is that the cellular base station or RTCM GPS receiver has been compromised.
 - 3.5.2. Hacker compromised TMS. This is for the case when the RTCMs are sourced by the TMS. Possible actions that lead to this state are described in the “Hacker compromised TMS” attack sub-tree.

Mitigations

Mitigations for the events/adversary activity listed above are listed in Table 43.

Table 43. Mitigation - RSU Outputs Incorrect RTCM Messages

Adversary Action Name	Possible Mitigation(s)
3.1 RTCM source signs with invalid certificate	1. RSU checks RTCM signature and does not output a RTCM if it doesn't pass this check.
3.2 RSU signs with invalid certificate	1. See corresponding entry 1.1 in the "RSU outputs incorrect SPaT" mitigations
3.3 Malware loaded on RSU	1. See corresponding entry 1.2 in the "RSU outputs incorrect SPaT" mitigations
3.4 RSU is misconfigured	1. See corresponding entry 1.3 in the "RSU outputs incorrect SPaT" mitigations
3.5 RTCM data is incorrect	1. Ensure RSU software employs input validation 2. See child attacks for mitigations
3.5.1 Hacker compromised RTCM server	1. Ensure RSU software employs input validation 2. See corresponding entry 1.4.1.2 in the "RSU outputs incorrect SPaT" mitigations, with TMS being replaced by RTCM server
3.5.2 Hacker compromised TMS	1. Ensure RSU software employs input validation 2. See corresponding entry 1.4.1.2 in the "RSU outputs incorrect SPaT" mitigations

Annex F Testing Resources [Informative]

This annex contains a list of resources for testing.

F.1 Existing Test Documentation

Table 44. Existing Test Documentation

Document Name, Date	Comment	Sponsor	Test Plan	Test Procedures	Test Cases	Test Log	Test Report
Test Plan for Connected Vehicle (CV) Pilots Phase 2 Interoperability Testing, May 15, 2018	Provided by J. Anderson, also D. Benevelli	FHWA	X	Data Collection	X	X	
Connected Vehicle Pilots Phase 2 Interoperability Test Test Report, November 9, 2018	Provided by J. Anderson	FHWA	X		X		X
Test Procedure for Verifying SPaT and MAP Messages, September 18, 2019	Provided by J. Parikh	CAMP		X			
SPaT Challenge Verification Document, October 30, 2017	Provided by J. Parikh	CAMP		X			
Test Readiness Review Checklist	Provided by J. Anderson. Useful for tracking/conducting test readiness review (TRR) which is the final go/no-go decision for conducting the test.	FHWA	X	X			
Interoperability Test Notebook	Provided by J. Anderson. Used to create physical notebooks for data collection and tracking of each test.	FHWA				X	
Interoperability Test Compiled Notebook	Provided by J. Anderson. Spreadsheet format to consolidate information collected from the notebooks.	FHWA				X	
Actual Run Order and Start Times	Provided by J. Anderson. Consolidated list of all test runs and in what order.	FHWA				X	
DRAFT Connected Vehicle Deployment Environment, August 2020	Provided by J. Parikh	CAT Coalition	X				

F.2 Example Usage of a Test Tool

The section contains an example usage of an OBU-based test tool, to verify that a broadcasted SAE J2735_202007 SPaT and MAP message conforms with the requirements of this CI Implementation Guide.

The diagram below shows the OBU-based Test Tool in relation to the project scope, indicated by the red arrow at left, and the OBU Test Tool log file at right:

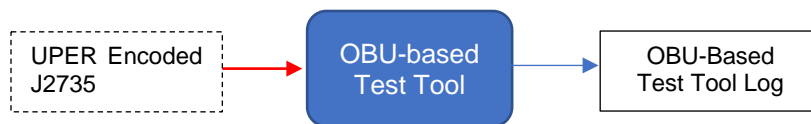


Figure 48. Example Testing Scope.

F.2.1 Description of OBU-Based Test Tool JSON Log

The OBU-based Test Tool's log file is a comma-delimited text file with each record containing 4 parts. Records in the log file are separated (terminated) with a line feed.

The four parts of the OBU-based Test Tool Log File are described below:

- a) **TimeStamp.** Epoch time to indicate message received time by the OBU.
- b) **MessageID.** The SAE J2735 MessageID to indicate message type: 18=MAP, 19=SPaT
- c) **Message.** A SAE J2735 SPaT or SAE J2735 MAP message represented in JSON Encoding Rules format. The JSON itself does not contain any line feeds or extra spaces. Because JSON contains commas and quotation characters, it is necessary to begin and end the JSON with a single-quote character.
- d) **SignedMessageIndicator.** 0 represents unsigned message, 1 represents signed message.

An example log file containing data format including the SPaT messages in JSON and imported into MS Excel is shown below.

A	B	C	D
1614109658855	19	'{"messageId":19 value:{"inter revision:52 status:"0000 moy:78440 timeStam:3 states:{"sigi	0
1614109658860	19	'{"messageId":19 value:{"inter revision:53 status:"0000 moy:78440 timeStam:3 states:{"sigi	0
1614109658865	19	'{"messageId":19 value:{"inter revision:54 status:"0000 moy:78440 timeStam:3 states:{"sigi	0
1614109658901	19	'{"messageId":19 value:{"inter revision:55 status:"0000 moy:78440 timeStam:3 states:{"sigi	0
1614109658905	19	'{"messageId":19 value:{"inter revision:56 status:"0000 moy:78440 timeStam:3 states:{"sigi	0
1614109658908	19	'{"messageId":19 value:{"inter revision:57 status:"0000 moy:78440 timeStam:3 states:{"sigi	0
1614109658912	19	'{"messageId":19 value:{"inter revision:58 status:"0000 moy:78440 timeStam:3 states:{"sigi	0
1614109658915	19	'{"messageId":19 value:{"inter revision:59 status:"0000 moy:78440 timeStam:3 states:{"sigi	0
1614109658919	19	'{"messageId":19 value:{"inter revision:60 status:"0000 moy:78440 timeStam:3 states:{"sigi	0
1614109658922	19	'{"messageId":19 value:{"inter revision:61 status:"0000 moy:78440 timeStam:3 states:{"sigi	0
1614109658926	19	'{"messageId":19 value:{"inter revision:62 status:"0000 moy:78440 timeStam:3 states:{"sigi	0
1614109658929	19	'{"messageId":19 value:{"inter revision:63 status:"0000 moy:78440 timeStam:3 states:{"sigi	0
1614109658933	19	'{"messageId":19 value:{"inter revision:64 status:"0000 moy:78440 timeStam:3 states:{"sigi	0

Figure 49. Example Log File Output.

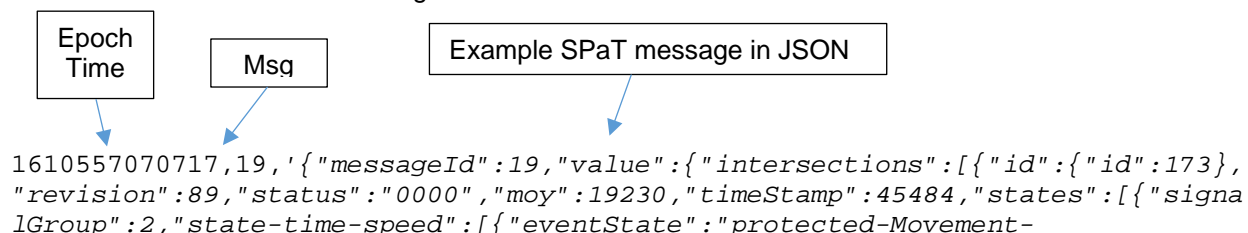
It should be noted that the JSON, shown in column C is not a complete message. The complete message is a long string.

F.2.2 Description of OBU-Based Test Tool JSON Log

An exploded view of the SPaT JSON contained in the log file is shown below:

It should be noted that, to reduce the logged JSON file size, there are no spaces in a record. Each record in the file ends with linefeed (new line). A log file contains both SPaT and MAP messages as being broadcast by an RSU. A post processing software separates the SPaT and MAP messages and saves them in separate files for parsing JSON and message processing for each intersection.

Example: OBU Test Tool logged data record for a SPaT message. The logged SPaT messages file contains all received SPaT messages.



```
Allowed", "timing": {"minEndTime": 34654, "maxEndTime": 35244}}]}], {"signalGroup": 4,
"state-time-speed": [{"eventState": "stop-And-Remain", "timing": {"minEndTime": 34711, "maxEndTime": 35301}}]}], {"signalGroup": 5,
"state-time-speed": [{"eventState": "stop-And-Remain", "timing": {"minEndTime": 34654, "maxEndTime": 34654}}]}], {"signalGroup": 6,
"state-time-speed": [{"eventState": "protected-Movement-Allowed", "timing": {"minEndTime": 34700, "maxEndTime": 35380}}]}]}]}], 0
```

Figure 50. Log File Entry SPaT JSON Encoding Rules.

Important: The logged messages in JSON above must reflect the same names as specified in the ASN.1 description of an SAE J2735_202007 SPaT message. An example of the ASN.1 for SAE J2735_202007 is shown below.

Example 1: Snippet of ASN.1 for LaneAttributes-Vehicle:

```
LaneAttributes-Vehicle ::= BIT STRING {
  -- With bits as defined:
  isVehicleRevocableLane      (0),
                                -- this lane may be activated or not based
                                -- on the current SPaT message contents
                                -- if not asserted, the lane is ALWAYS present

  isVehicleFlyOverLane        (1),
                                -- path of lane is not at grade

  hovLaneUseOnly              (2),
  restrictedToBusUse           (3),
  restrictedToTaxiUse          (4),
  restrictedFromPublicUse      (5),
  hasIRbeaconCoverage         (6),
  permissionOnRequest         (7) -- e.g., to inform about a lane for e-cars

} (SIZE (8,...))
```

Example 2: Snippet of ASN,1 for TimeChangeDetails:

```
TimeChangeDetails ::= SEQUENCE {
  startTime    TimeMark      OPTIONAL,
               -- When this phase 1st started

  minEndTime   TimeMark,
               -- Expected shortest end time

  maxEndTime   TimeMark      OPTIONAL,
               -- Expected longest end time

  likelyTime   TimeMark      OPTIONAL,
               -- Best predicted value based on other data

  confidence   TimeIntervalConfidence OPTIONAL,
               -- Applies to above time element only

  nextTime     TimeMark      OPTIONAL
               -- A rough estimate of time when
               -- this phase may next occur again
               -- used to support various ECO driving power
               -- management needs.
}
```

Example 3: Snippet of ASN,1 for TimeMark:

```
TimeMark ::= SEQUENCE {
  year        Year,          -- BCD coding of A.D.    2 octets
  month       Month,         -- BCD coding of Month,  1 octet
  day         Day,           -- BCD coding of Day,    1 octet
  summerTime  SummerTime,
```

```

holiday      Holiday,
dayOfWeek    DayOfWeek,
hour         Hour,          -- BCD coding of Hour,    1 octet
minute      Minute,        -- BCD coding of Minute, 1 octet
second      Second,        -- BCD coding of Second, 1 octet
tenthSecond TenthSecond   -- units of 100 millisecond, 1 octet
}

```

For complete detail refer to: SAE J735-201603 Final ASN specification.

F.2.3 Description of OBU-Based Test Tool JSON Log

The following example shows test tool logged data for a MAP message.



Similar to the SPaT message, the MAP message also contains epoch time, message id, MAP message (in italics), and signed message indicator.

Annex G

User Requests [Informative]

This annex identifies needs, requirements, and design details that were identified and considered by the CI Committee or its task forces for this CI Implementation Guide, but were not included. The rationale on why these needs, requirements, and design details were not included is also provided. This section is included for consideration for future editions of the CI Implementation Guide.

G.1 User Requests - Needs

This sub-section identifies user needs that were identified and considered by the CI Committee or its task forces.

G.1.1 Mobility Applications

The CI Committee primarily did not consider user needs for mobility applications for this version of the CI Implementation Guide. As stated in Section 2.3, only user needs to support the RLVW application were considered due to time and resource constraints. Needs to support SPaT-based and MAP-based safety and mobility applications were considered if the requirements to satisfy those needs and the design to fulfill those requirements can be completely defined within the project schedule.

G.1.2 Queue Information at an Intersection

The CI Committee considered a need to provide vehicle queue data at an intersection. This information is used by mobility applications such as an eco-driving application. However, additional infrastructure equipment, such as detectors, are needed by IOOs to provide more reliable data. The SPaT/MAP Task Force decided there was insufficient time to address this need at this time.

G.1.3 Indication of Pedestrians or Bicyclists in a Crosswalk

The CI Committee considered a need to provide the presence of pedestrians or bicyclists in a crosswalk at an intersection. While this information can be used by OBU applications for safety, additional infrastructure equipment such as detectors are needed by IOOs to provide data with a high level of confidence. The SPaT/MAP Task Force decided there was insufficient time to address this need at this time.

G.1.4 Confidence Factor and Likely Time

The CI Committee considered a need to provide a confidence factor and likely time for the time of change details as part of the signal phase and timing information provided by a connected intersection. The user need for confidence factor was expressed as follows. "A connected intersection needs to provide a confidence indicator for the predicted time when the current signal interval (state) for each movement at the intersection will change so an application can provide the proper warnings, information or guidance to the driver or VRU. At any point in time, the future signal interval of an intersection is subject to factors that may be unknown to a traffic signal controller such as the future intersection demand, a preemption operation, or a change in timing plan from a management system. Some applications, such as safety applications, depend on timing information with high certainty. Other applications may function adequately with less certain timing information. A confidence factor helps applications interpret the data."

Note, a requirement for confidence was also developed as follows, "A connected intersection shall provide a confidence indicator for the predicted time when the current signal interval (state) for each movement at the intersection will change so an application can provide the proper warnings, information or guidance to the driver or VRU. This confidence indicator is used for mobility applications and not safety applications."

However, for safety applications, the time-to-change information needs to be near, if not at, 100 percent confidence, excluding unexpected events such as preemption operation. There was discussion that confidence factor and likely time could be used by supervisory traffic control systems for statistical

information on the operation of the TSC infrastructure, however there was no consensus on a scheme to calculate this information in the TSC infrastructure reliably.

G.1.5 Signal Priority and Preemption

The CI Committee considered a need to provide the status of signal priority or preemption requests at an intersection. A need statement could read: "A connected intersection needs to provide information about current priority or preemption requests so an application can provide the proper warnings, information, or guidance to the vehicle. The RL/VW implementation should neither preclude SRM and SSM nor SPaT messages and signal timing changes based on these messages." The CI Committee decided that there was insufficient time and resources to address this need at this time.

G.1.6 Advisory Speeds

The CI Committee considered a need to provide advisory speeds for a movement at an intersection so an application can provide appropriate information or guidance to a driver. This need would also partially satisfy the needs of eco-driving applications. However, the IOOs did not currently have enough experience from with field testing to define requirements and testing approaches.

G.1.7 Misbehavior Reporting by OBUs

The CI Committee considered a need, "A connected intersection needs to provide a mechanism to allow OBUs to report incorrect data from the infrastructure so that faulty CI messages do not compromise applications or user actions." However, the CI Committee agreed this need is out of scope at this time and could require a large amount of effort. The CI Committee also noted that an OBU can report that it sees a conflict between the message and what it sees (e.g., via an on-board camera), but this conflict is not addressed by any group/standard right now.

G.1.8 Misbehavior Reporting by IOO Field Devices

The CI Committee considered a need, "A connected intersection needs to provide a mechanism to allow IOO field devices to report incorrect data from the infrastructure so that faulty CI messages do not compromise applications or user actions." However, the CI Committee agreed this need is out of scope at this time and could require a large amount of effort. The CI Committee also noted this need is not addressed by any group/standard right now.

G.1.9 Levels of Testing

The CI Committee considered a need, "The CI test methodology needs to define Levels of Testing." However, the CI Committee agreed there was insufficient time to address this need at this time.

G.2 User Requests - Requirements

This sub-section identifies requirements that were identified and considered by the CI Committee or its task forces, but are not addressed in this CI Implementation Guide.

G.2.1 Quality Assurance

The CI Committee considered requirements on Quality Assurance. However, the SPaT/MAP Task Force decided that there was insufficient time and resources to address these requirements at this time.

- **SPaT Message Quality Assurance.** A connected intersection shall verify that the SPaT message currently being broadcast is compatible with what the TSC infrastructure is commanding and with the physical indications being displayed at the intersection.
- **MAP Message Quality Assurance.** If the MAP message currently being broadcast and the MAP message previously broadcast have the same revision number, a connected intersection shall verify that they are identical except for any time stamp.
- **SPaT Message Reset.** After a connected intersection has set the intersection status to indicate no valid SPaT data based upon an anomaly while verifying the SPaT message, the connected

intersection shall not broadcast movement state and timing data again without human verification that the SPaT message has been corrected.

- **MAP Message Revisions.** A connected intersection shall not broadcast a MAP message with a different revision number from the previously broadcast MAP message without human verification that the change is intentional.

G.2.2 Computed Lane – Scaling

The CI Committee considered requirements for scaling (X-axis and Y-axis), however, there were no known implementations that used scaling at the time, and the design details on how to implement it and how a computed lane with scaling would look was unclear. The requirement that was developed, was "A connected intersection shall provide a scaling factor along the x-axis (or y-axis) for a computed lane relative to the first node point of the referenced lane. The design detail was, "If the computed lane is a different scale from the referenced lane, the scale along the x-axis (east-west) (or y-axis (north-south)) is represented as *scaleXaxis* (or *scaleYaxis*) (*DE_Scale_B12*) and can be found under the data frame *DF_ComputedLane* in the *MSG_MapData* message in *SAE J2735_202007*. The scale factor is measured in 0.05 percent increments with positive values indicating that the computed lane is larger than the referenced lane."

G.2.3 No SPaT Available

The CI Committee considered a requirement, "A connected intersection shall indicate when no valid SPaT information is available. SPaT information is considered not valid under the following conditions:

- If the connected intersection is transmitting SPaT messages not compatible with what the TSC infrastructure is commanding or with the physical indications being displayed at the intersection."

This requirement would allow an enhanced OBU/MU to report discrepancies between the signal indications "seen" by the OBU/MU and compare the signal indications with the movement state(s) reported in the SPaT messages. However, this capability does not currently exist, so this particular requirement is not addressed in the CI Implementation Guide.

G.2.4 TSCBM

Because there was insufficient CV object support in NTCIP 1202 v02, TSCBM was a solution taken by manufacturers to support various CV deployments during the SPaT challenge and federal projects. However, the intent of *NTCIP 1202 v03A* was to address the deficiencies in v02. Currently, we recognize that there are even more clarifications are necessary to ensure an interoperable environment and have taken the steps to recommend clarifications to the standards (among them NTCIP 1202) in the CI Implementation Guide. These clarifications in the CI Implementation Guide will be forwarded to the associated standards working groups for further discussion and adoption.

To ensure interoperability, it is the SDO's vision to update the *NTCIP 1202 v03A* standard using clarifications in the CI Implementation Guide and sunset use of TSCBM in future projects. Existing validation sites using TSCBM may continue use of TSCBM for the validation phase of the CI project. The CI WG does not recommend deploying TSCBM at new locations.

G.3 User Requests - Design Details

This sub-section identifies design details that were identified and considered by the CI Committee or its task forces, but are not addressed in this CI Implementation Guide.

G.3.1 Failure Flash

The CI Committee considered a requirement, "A connected intersection shall indicate whether the intersection is in a signal flash condition invoked outside of the TSC infrastructure (e.g., a fault, toggle switch, police panel)." While the TSC infrastructure may be aware of several forms of failure flash, it may not be aware of all forms of failure flash, depending on how the connected intersection is wired. For

example, the TSC infrastructure may not be aware of a cabinet flash or a conflict flash. Separate wiring may be needed so that the RSU or the TSC infrastructure is aware of a cabinet/conflict/failure flash. The design details on when the TSC infrastructure is in failure flash needs to be defined in more detail, including guidance on how to be more complete in reporting all forms of failure flash.

G.3.2 Operational Logging – TSC Infrastructure

The CI Committee considered a requirement, "The TSC infrastructure shall record salient events in a non-volatile log. This includes logging of security events such as authentication failures, logs of changes to its configuration." While general design details were provided for this requirement, more exact design details are needed to avoid ambiguity. However, the Traffic Controller Issues Task Force decided there was insufficient time to fully address the design details at this time.

G.3.3 Connections

Showing a connection in the MAP message between an egress lane and an ingress lane of an adjacent intersection allows an OBU/MU to know the intersection reference identifier of the next intersection it will encounter. This can aid the OBU/MU in situations where it may be in range of broadcasts from multiple connected intersections. If the connection is provided, the Remote Intersection Reference Identifier for the downstream intersection is needed. However, there was insufficient time and resources to fully develop implementation guidance on how to provide these connections.

G.3.4 Test Cases

The CI Committee considered developing a complete set of test cases for a fully conformant connected intersection, including security. However, given the project and schedule constraints, the CI Committee deferred developing test cases to fully validate and verify the CI Implementation Guide. However, the CI Committee did develop Section 5, Connected Intersection Testing [Informative], which contains test cases to verify a subset of the SPaT and MAP messages as part of the CI Validation Site Testing that was conducted in Spring/Summer 2021.

G.3.5 Security Models

Consider which SNMP security models are permissible, in coordination with NTCIP and with any RSU standard updates.

Annex H Recommendations to SDOs [Informative]

This annex summarizes comments and recommendations by the CI Committee or its task forces to Standards Developments Organizations on existing standards that are referenced by this CI Implementation Guide.

H.1 SAE Core Technical Committee - SAE J2735

This section identifies comments and recommendations by the CI Committee for *SAE J2735_202007*, V2X Communications Message Set Dictionary.

H.1.1 DE_TimeMark

The CI Committee recommends that the description of DE_TimeMark be improved in two ways.

- 1) To indicate when it is in the current or next hour (i.e., if TimeMark > current tenths of a second into the current hour, then TimeMark is in the current hour; if TimeMark is < current tenths of a second into the current hour, then TimeMark is in the next hour) and can include more detail regarding what to do when a leap second occurs.
- 2) SAE J2735_201603 version describes DE_TimeMark as "-- Tenths of a second in the current or next hour -- In units of 1/10th second from UTC time." However, *SAE J2735_202007* removed the first phrase, "tenths of a second in the current or next hour," thus introducing an ambiguity because it no longer indicates the reference point - is it tenths of a second from the top of the hour or from the current UTC time, which is always moving. The CI Committee recommends restoring the deleted phrase.

This is what currently appears in *SAE J2735_202007*:

```
TimeMark ::= INTEGER (0..36111)
-- In units of 1/10th second from UTC time
-- A range of 0~35999 covers one hour
-- The values 36000..36009 are used when a leap second occurs
-- The values 36010..36110 are reserved for future use
-- 36111 is to be used when the value is undefined or unknown
-- Note that this is NOT expressed in GPS time or in local time
```

H.1.2 DF_MovementEventList

The CI Committee requests a minor change in the language describing DE_MovementPhaseState. The language for DE_MovementPhaseState is described as a present state and not a future state, specifically, "The DE_MovementPhaseState data element provides the overall current state of the movement...." However, DF_TimeChangeDetails states 'The StartTime element is used to relate when the phase itself started *or is expected to start*. This in turn allows the indication that a set of time change details *refers to a future phase*, rather than a currently active phase.' This implies that the DE_MovementPhaseState associated with the time change details could also refer to a future state of the movement.

The CI Committee proposes to use DF_MovementEventList to present the current movement details but also the details for the next movement (interval). To support a future state, the CI Committee requests that the text be updated to, "The DE_MovementPhaseState data element provides the overall state of the movement...."

H.1.3 DE_IntersectionStatusObject

The CI Committee has comments on the following bits defined for DE_IntersectionStatusObject:

- *fixedTimeOperation* (5) and *trafficDependentOperation* (6) are mutually exclusive. The CI Implementation Guide populates both bits, but *trafficDependentOperation* is not needed.
- *recentMAPmessageUpdate* (10) and *recentChangeInMAPAssignedLanesIDsUsed* (11) do not define what is considered to be a recent update or change. To be useable, this would need to be defined. For safety, the CI Committee recommended that connected intersections always set these bits to 1.

For backwards compatibility, no change is needed unless the bits are needed.

H.1.4 DF_NodeAttributeSetLL

The CI Committee notes that for dElevation, the note states that "--A value added to the current Elevation --at this node from this node onwards, in 10cm steps." The CI Committee believes this may be a typo and should be in **1cm** steps. The CI Committee requests a clarification.

This is what currently appears in *SAE J2735_202007*:

```
NodeAttributeSetLL ::= SEQUENCE {  
  ...  
  dElevation Offset-B10 OPTIONAL,  
  -- A value added to the current Elevation  
  -- at this node from this node onwards, in 10cm steps  
  -- elevations between nodes are a linear taper between pts  
  -- the value of zero shall not be sent here
```

H.1.5 DE_RoadRegulatorID

To assign a unique identifier for each signalized intersection in North America, the CI Committee attempted to develop a scheme for assigning road regulator identifiers using existing jurisdiction codes so a registration authority would not be needed. Unfortunately, the CI Committee was unable to find a scheme that would fit within the 16-bit integer defined for DE_RoadRegulatorID. It is recommended that DE_RoadRegulatorID be enhanced or supplemented. For example, consider a 2-part identifier consisting of the ISO country code plus "." plus a country specific jurisdiction code. For the United States, consider using the Geographic Names Information System feature ID for this code.

H.1.6 DF_TimeChangeDetails

The CI Committee requests clarifying the use of startTime. The Use of DF_TimeChangeDetails defines StartTime as, "The StartTime element is used to relate when the phase itself started or is expected to start. This in turn allows the indication that a set of time change details refers to a future phase, rather than a currently active phase." This definition is preventing interoperability as it allows StartTime to be a point in the past or a point in the future. Note that TimeMark can be in the future or in the past, so it becomes ambiguous whether the time mark is referring a time in the past hour, the current hour, or the next hour.

The CI Committee recommends updating the definition of startTime to be consistent with all other uses of DE_TimeMark in DF_TimeChangeDetails, i.e., only refer to a time in the future. Thus startTime would only be used for intervals in the future, never for the interval currently timing, contrary to the ASN.1 comment.

If there is a need to represent a point in the past, a different (optional) data element should be added to DF_TimeChangeDetails.

H.1.7 MAP Message

Recognizing transport message size limitations, the CI Committee recommends updating the MAP message to allow for larger MAP messages, potentially by allowing one MAP to be sent in multiple MAP messages.

Although the MAP message for most connected intersections does not exceed the message size limitations allowed by the transport used, there are some intersections where the MAP message size may need to exceed those limitations to fulfill the requirements in this CI Implementation Guide. Examples of requirements that may result in large MAP message sizes include the following:

- 3.3.3.4.1.7 - 3.3.3.4.1.9, which requires that all permitted vehicle lanes, crosswalk lanes and pedestrian landings be identified
- 3.3.3.4.1.17, Advanced Notification - Ingress Vehicle Lane, which requires that each ingress vehicle lane extend a minimum distance from the first node point of the lane
- 3.3.3.4.1.20, Maximum Distance between Nodes, which defines the maximum allowable distance between the centerline of a lane and the straight line between two consecutive node points

H.1.8 Backwards Compatibility

The CI Committee respectfully asks SAE not to make changes to a *SAE J2735_202007* data element that would break backwards compatibility. For example, if a new data element *DE_TimeMark2* was created with the changed meaning of 36001, it would not break backward compatibility. The receiving entity would know which version of timemark was being used and interpret it safely. Then *DE_TimeMark* could be deprecated.

H.2 NTCIP Actuated Signal Controllers (ASC) Working Group

This section identifies comments and recommendations by the CI Committee for *NTCIP 1202 v03A*.

H.2.1 Protected / Permissive Movements

There is a question if the logic for resolving protected versus permissive movement as currently stated in *NTCIP 1202 v03A* is correct. *NTCIP 1202 v03A* looks at the protected turn phase channel and the opposing through phase channel. If the protected turn phase is green and the opposing through phase is red, it says it is protected, which would be true. If the protected turn phase is green and the opposing through phase is green, it says it is permissive, but that situation can never exist. The protected turn phase and opposing through phase can never be green at the same time.

H.2.2 Hard Flashing Operation

The CI Committee recommends that object definitions be created to include configuration of signal output status so a traffic controller can broadcast signal head status when under hard flash operation. See A.2.1.6, Hard Flashing Operation. Flash color is often hardwired in the cabinet using jumpers or plugs such that the controller is unaware of what colors are flashing.

H.2.3 Dynamic AWEG Decisions

The CI Committee recommends that object definitions be created to define for the placement of detection zones at an intersection as well as decision support options for dynamic AWEG decisions. See A.2.1.10, Output Mapping.

H.2.4 Output Mapping

The CI Committee recommends that object definitions be created to establish lookup tables that allow the traffic controller firmware to have an accurate mapping of phase and overlap outputs relative to the lane identifier for a lane and the allowable maneuver basis. See A.2.1.10, Output Mapping.

H.2.5 Additional SPaT Elements

The CI Committee recommends that object definitions be created to support additional data elements required to generate a *SAE J2735_202007* SPaT message. Table 8 identifies several data elements that are required for the SPaT message that are not currently supported by *NTCIP 1202 v03A*. Those data elements are *DE_RoadRegulatorID*, a data instance called the *startTime*, and state and timing information for the next interval (if known). The CI Committee recognizes that the *startTime* was deliberately not supported because the definition of *startTime* was ambiguous at the time, but hopefully, the use of *startTime* defined in this CI Implementation Guide provides sufficient clarity.

H.2.6 SPaT Data Tables

The CI Committee asks if the ASC Working Group would consider restructuring their SPaT data tables to 1) be compatible with the *SAE J2735_202007* SPaT message structure and 2) to provide a means to send up to 16 current and future interval states for each signal group rather than just the current state. The current *NTCIP 1202 v03A* data table structure provides interval state at the movement/maneuver level as well as at the channel (=SignalGroupID) level, while *SAE J2735_202007* only can provide it at the signal group level. 3) *SAE J2735_202007* already provides a means to broadcast 16 current and future interval states for each signal group, while *NTCIP 1202 v03A* only allows for the current state. The RLVW ConOps and Requirements indicate a need for knowing the yellow timing while the light is still green and need to use this *SAE J2735_202007* allowed feature.

H.3 NEMA TS2 Working Group

There is a risk a DC isolator failure may remove controller awareness of flashing conditions. The CI Committee recommends the NEMA cabinet standards group consider the addition of MMU/CMU interlock inputs (similar to RR preemption interlock circuitry) to ensure controller awareness of flashing operation. See A.2.1.6, Hard Flashing Operation.

H.4 ATC Joint Committee/ITS Cabinet Working Group

There is a risk a DC isolator failure may remove controller awareness of flashing conditions. The CI Committee recommends the NEMA cabinet standards group consider the addition of MMU/CMU interlock inputs (similar to RR preemption interlock circuitry) to ensure controller awareness of flashing operation. See A.2.1.6, Hard Flashing Operation.

Annex I

RLVW Deployment - Practitioner Approach [Informative]

I.1 Introduction

The purpose of this annex is to provide guidance on approaches, resources and best practices for how to deploy and operate connected intersections to support RLVW applications. These considerations will complement the discussion of the system needs, system requirements and design considerations covered in the main part of this document.

This section will discuss the following topics:

- What are expectations for the CI with deployed RLVW applications and how these goals can be achieved.
- How to deploy a CI on a new intersection or upgrade existing intersections to support RLVW application.
- What are important resources, approaches and best practices which an agency can follow to deploy and maintain a CI over long term.

The main audience for this section includes transportation agencies, IOOs, infrastructure designers, system integrator, deployers and system operators. This section may also be of interest to manufacturers of roadside equipment, vehicle manufacturers (OEMs) and other parties involved in the design of the components which will be used as part of a CI and support RLVW applications.

This section is not intended to be a tutorial on the deployment of a CI. Rather we assume that the reader has understanding of the CV technology, its basic approaches and building blocks, and some experience in planning and deploying of the CV infrastructure. Section I.5 includes links to additional documents which can help the reader to learn about CV.

In the context of this section, CI refers to a general CV system at an intersection which is designed, implemented, validated and operated to conform to CTI 4501. The CI is expected to support the RLVW application as discussed in the main section of the document. Additionally, the CI may have the capability to support other CV applications, which are outside the scope of this guidance document, but might be discussed elsewhere.

I.1.1 Expectations for the RLVW System Performance

This section discusses general expectations from system users and how these goals can be attained by a CI supporting RLVW applications.

I.1.1.1 Delivers Expected Performance and Accuracy

The CI is expected to support a wide range of safety applications including RLVW, AGP and serve as a foundational element for various intersection-based CV systems. To fulfill its intended purpose, the CI must fulfill specific performance, reliability, and accuracy requirements. Meeting these criteria will ensure that vehicle safety applications which are expected to use information provided by the CI, can rely on the CI data to the same extent as humans rely on accuracy and performance of traffic signals.

Once a CI is deployed, a series of validation tasks need to be performed to ensure that the system adheres to the requirements and design guidelines. Subsequently, the CI system needs to be monitored to ensure that it continues to operate within acceptable performance tolerances.

While this document does not define or specify the service level expectations and performance criteria for the on-going system operation, they may be defined in agency performance guidelines or developed over

time through national agency collaboration and explicit performance agreements between CI system operators, security credential providers, and other stakeholders.

I.1.1.2 RLVW is Interoperable

It is anticipated that CIs constructed in compliance with CTI 4501 will attain a significant level of interoperability. This implies that an application designed and tested on a CI system in one location will exhibit similar performance when interacting with CI systems deployed in other locations. The ultimate goal is to achieve robust interoperability among all CI systems deployed throughout the North America (including Hawaii, Guam, Puerto Rico) and maintain this level of compatibility over an extended period.

Effective change management will be a crucial factor in attaining and sustaining interoperability. Once the CI system is validated and enters operation, it will require regular maintenance, updates, and occasional component upgrades. As technology and technical requirements continue to evolve, introduction of new features should not hinder existing users from utilizing the system. Simultaneously, the CI should enable the adoption of the latest CTI specifications and facilitate a smooth transition, ensuring that CI services remains available to the majority of system users.

I.1.1.3 Secure

Security is of importance for the CI as it assures confidence and trust in the CI information shared with vehicle users. Sections 2.4.4, 3.3.4, and 4.3.4 of CTI 4501 respectfully addresses security needs, requirements, and design approaches specific to the CI system. As an integral part of an operating agency's infrastructure, the CTI security requirements must be aligned and coordinated with the security approaches employed by the system operator for all of their other deployed systems.

I.1.1.4 Sustainable and Reliable

The CI is expected to be sustainable and reliable. Throughout many decades, drivers have placed their trust in traffic signals at intersections. Similarly, we expect that the safety applications integrated into connected and automated vehicles will be able to depend on the data and services provided by the CTI.

System reliability depends on capability of the underlying CI components as well as organizational capabilities to support and maintain the system. In the latter case, road maintenance and other maintenance activities conducted by the agency, will require regular adjustments to system parameters (e.g. MAP files). The consistency of SPaT and MAP messages, and their consistency and accuracy to describe existing road conditions is a challenge which must be addressed.

Managing and supporting updates, particularly software updates, for the CI infrastructure will present another challenge. A significant portion of the system's features are implemented in software. The ability to facilitate software updates to address existing issues and introduce new features across different CI components is crucial for ensuring the system's longevity. However, it is equally important that these software updates maintain the integrity, interoperability, and consistency among all CI components.

As more RLVW systems are deployed, a deeper understanding of sustainability and reliability will emerge. Additionally, we anticipate that improvements in equipment reliability and system management will lead to a high level of proficiency, making CI extremely reliable.

I.2 Architectural Views

The purpose of this section is to use architecture diagrams to showcase system, services and functions required to deploy and operate the CTI. We also highlight that a deployer can contemplate a variety of architectural options when implementing the CI system.

Two views will be presented: the Services View and the Communication View. These diagrams are intended to illustrate the elements of the system's architecture, relationships among these elements and demonstrate different communication paths to link the system together.

We acknowledge that CV systems deployed in diverse infrastructure environments have evolved along slightly different paths and adopted varied architectures to adapt to existing resources and capabilities. As a result, the architectural views presented below are intended to illustrate the necessary services, functionality, and typical data flows. These diagrams do not impose any specific architecture but rather aim to demonstrate the entire scope of the implementation which can adequately support the scope of the CTI4501 requirements.

I.2.1 Services View

The Services View architecture is shown in Figure 52. It includes architecture elements which are expected when the CI system is fully implemented with the capabilities known at the present time.

The diagram partitions the CI system into three layers: External Networks, Center Network and Field Network. Within each layer, functions and services are grouped and represented by specific icons that illustrate the various functionalities and services used in the CI system. The objective is to identify the functions of these elements supporting system operation, configuration, monitoring, and information distributions.

The diagram below does include OBU representation to highlight that OBUs are critical to the integration and some OBUs managed by IOO (e.g. fleet vehicles) may utilize elements of the same infrastructure for security, firmware updates, etc. However, OBU support of RLVW applications and integration into the CI system is outside of the scope of this document.

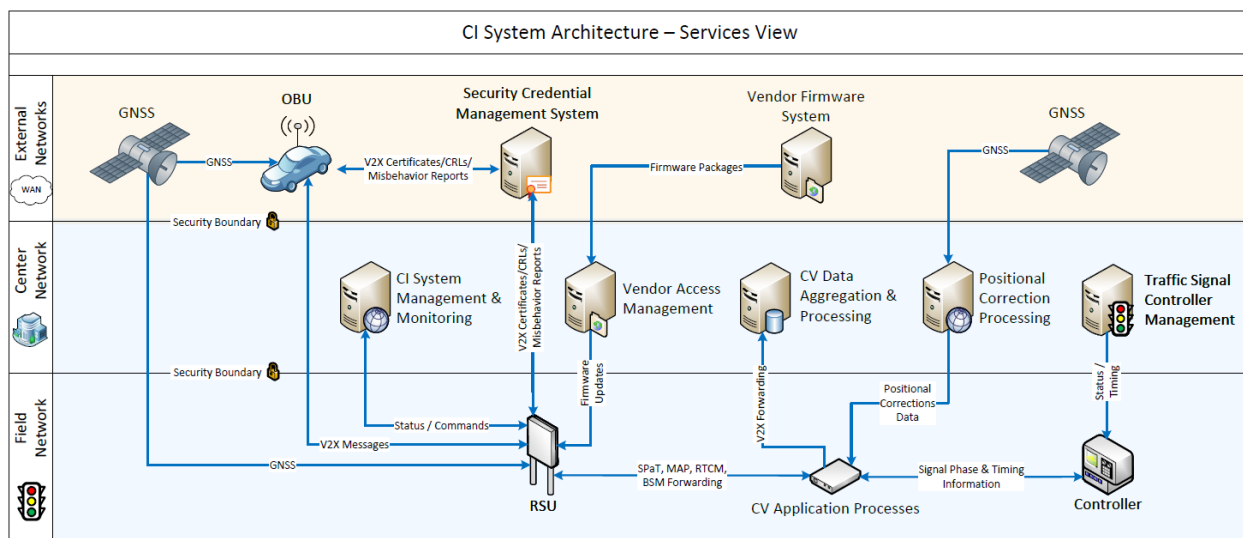


Figure 52. CI System Architecture – Services View.

Table 45 below discusses main functionality and services provided by the various elements presented in Figure 52.

Table 45. Services and Functionality Represented on Figure 52.

Component	Provided Services / Functionality
Field Network	Encompasses systems and services deployed in the field.

Component	Provided Services / Functionality
Controller (Traffic Signal Controller or TSC)	<ul style="list-style-type: none"> Operational controller of traffic signals at an intersection. This is the source of signal phase and timing information for the SPaT messages. Some TSC implementations may also support encoding SPaT into J2735 format, and store and encode MAPs into J2735 format. Having the TSC support these functions may require a deployment practitioner to change the configuration of an RSU but will not significantly alter the system architecture on Figure 52
CV Application Processes	<ul style="list-style-type: none"> Supplemental processing required to facilitate data exchanges between TSC and RSU, and Positional Reference System and RSU. Receives, processes BSM messages and converts them into TSC inputs to support AGP. Receives RTCM messages from Positional Corrections Processing (i.e. GNSS, CORS or Positional Reference System), processes/converts and forwards them to the RSU. Stores and converts MAP messages for the RSU. Converts legacy TSCBM to the required SPaT format. May manipulate TSC timing, perform adaptive SPaT computations, and etc. Maintenance of RSU configuration/databases <p>Additional notes:</p> <ul style="list-style-type: none"> CV Application Processes may be implemented in the External Control Local Application (ECLA) processor The combination of TSC and ECLA is referred in the CTI 4501 as the Traffic Signal Controller Infrastructure. The ECLA may be utilized to support more customized and advanced data communication and conversion. It may support interface to “legacy” TSCs and RSUs. Over time, some of the CV Application Processes may be incorporated into TSC or RSU.
RSU (Roadside Unit)	<ul style="list-style-type: none"> Transmission/reception of V2X messages (i.e. SPaT, MAP, BSM, RTCM) at an intersection. Digital signing/verification of V2X message security. Interface to TSC (directly or via ECLA) to receive signal phase status and timing information. Interface to receive RTCM corrections. BSM message forwarding to a ECLA or TSC as well as to the CV Data Aggregation & Processing services. Storage of MAP messages (except when MAPs are stored elsewhere, i.e., ECLA, TSC or TMC)
Center Network	Comprised of systems and services operated within the backoffice network
Traffic Signal Controller Management	<ul style="list-style-type: none"> Agency control over TSC system. Operational system health monitoring, outage detection, data collection, timing plan and configuration management, signal coordination, etc. This may be part of an Advanced Traffic Management System (ATMS).
Positional Correction Processing	<ul style="list-style-type: none"> Agency control over processing of the GNSS data to produce required RTK/RTCM data for the field segment of the CI system. An agency managed non-localized CORS system may be viewed as an example.

Component	Provided Services / Functionality
CI System Management and Monitoring	<ul style="list-style-type: none"> Agency control over CI system. RLVW application performance monitoring. Exception detection due to hardware/software failures. System configuration management, backup, and restore.
Firmware Management	<ul style="list-style-type: none"> Agency control over software provisioning and updates for RSUs, ECLAs and other roadside components.
CV Data Aggregation and Processing	<ul style="list-style-type: none"> Collection of CV data (via BSM forwarding) from the Field Network, aggregation, data filtering, analysis, event extraction, performance reporting. May be used for CV data sharing/dissemination with other internal/external endpoints. Example implementation is FHWA Operational Data Environment project.
MAP Management	<ul style="list-style-type: none"> Creation and distribution of MAP messages to RSUs/ECLAs. MAP message creation and digital signing may be done as part of V2I System Management and Monitoring.
External Networks	All systems and services external to the system maintained by the infrastructure owner and operator and required for the RLVW system.
Security Credential Management System	<ul style="list-style-type: none"> Provisioning of V2X certificates Delivery of certificate updates, CRLs and reception of misbehavior reports. Monitoring of CI system compliance to security practices.
Vendor Firmware Systems	<ul style="list-style-type: none"> Vendor/external resources providing software repository for updates to V2X systems (RSU, ECLA, etc.) required for CI system operation. May also support OBU updates.
GNSS	<ul style="list-style-type: none"> External source of GNSS position and GNSS position corrections providing continuous GNSS and RTK/RTCM data for the CI system. The GNSS is used for determining position and precise timing by some field CI components, e.g., RSUs. The RTK/RTCM is used by RSUs to broadcast position correction messages.
In-vehicle On-board unit (OBU)	<ul style="list-style-type: none"> OBUs will exchange V2X messages with RSU in order to utilize CI system capabilities. OBUs managed by an agency may be used for CI system monitoring. OBUs may utilize agency Firmware Management service and Security Credential Management System service.
Security Boundary	<ul style="list-style-type: none"> A security/control service within agency for field devices for communication to approved external resources e.g., SCMS, CORS, etc. Secure communication between agency sub-networks as well as separation from external internet network. Establishes communication policies and control point for data exchanges between networks and sub-domains.

Table 46. Interconnections on Figure 52.

Flow label	1st end	2nd end	Description, Examples of data
Signal Phase & Timing Information	Controller (Traffic Signal Controller)	CV Application Processes	<ul style="list-style-type: none"> Signal status and timing information generated by the Controller is used to create SPaT messages.

Flow label	1st end	2nd end	Description, Examples of data
SPaT, MAP, RTCM, BSM Forwarding	CV Application Processes	RSU	<ul style="list-style-type: none"> • SPaT, MAP, RTCM messages if CV Application Processes is used to create them. Otherwise, this flow passes through to the RSU where the messages are generated and transmitted by the RSU • Information extracted from processed BSMs and sent to the Controller for the AGP application.
Signal / Timing	Traffic Signal Controller Management	Controller	<ul style="list-style-type: none"> • Controller timing plans, controller databases, settings, events.
GNSS	GNSS	Position Correction Processing	<ul style="list-style-type: none"> • Positional correction information collected from CORS before it is processed into RTCM.
Positional Corrections data	Position Correction Processing	CV Application Processes	<ul style="list-style-type: none"> • Positional correction information filtered and tailored to the CI deployment footprint.
V2X Forwarding	CV Data Aggregation & Processing	CV Application Processes	<ul style="list-style-type: none"> • CV messages and other data collected from RSUs, processed by the CV Application Processes and sent to data analytics.
Firmware Packages	Vendor Firmware System	Vendor Access Management	<ul style="list-style-type: none"> • Entire range of software updates, patches, new software passed from the vendor to the agency's Vendor Access Management.
Firmware Updates	Vendor Access Management	RSU	<ul style="list-style-type: none"> • Approved software updates, patches to be applied to RSUs and other field devices.
V2X Certificates/ CRLs, Misbehavior Reports	Security Credential Management System	RSU, OBU	<ul style="list-style-type: none"> • Certificates, CRLs, misbehavior reports and other security information. • Similar types of information may be exchanged between SCMS and RSUs, and SCMS to OBUs, however, the content of the data flows is different.
Status, Commands	CI System Management & Monitoring	RSU	<ul style="list-style-type: none"> • Status information and control commands use to monitor and manage the CI system.
V2X Messages	OBU	RSU	<ul style="list-style-type: none"> • V2X messages e.g., SPaT, MAP, RTCM and BSMs exchanged between RSU and OBU.

The Services View provides a “typical” view of the architecture system. The view is intended as a guidance to help an agency to define their own implementation. Though the diagram resembles physical implementation of the system, its focus is on services and functions which are organized, grouped and identified by an icon.

Some of the earlier deployments started with much simpler architecture where some functions were performed manually or in a simplified manner. This allowed an agency to utilize existing resources to gain experience with the system before deciding to scale up and determine investment strategy for the more complex system.

In the actual implementation, certain services may be integrated or combined with other elements. For example:

- ECLA functions may be integrated into TSC or RSU.

- MAP messages may be signed at the TMC as opposed to an RSU
- RTCM messages may come from an external network server, may be served by the agency-maintained CORS network or may be generated by a local NTRIP receiver feeding directly into the RSU.
- Firmware updates may be handled for RSUs from vendor servers or can be provided by the agency IT groups as part of centralized asset management.

In all these variants the implemented functionality is more important than adherence to a specific diagram or view. Another consideration is the agency capability to scale up the deployment and while actively monitoring the CI to achieve target performance, security and reliability objectives.

It is important to recognize that in the long-term, implementation of the CI is not limited to the deployment of field devices (i.e. RSU, TSC) and certain services (e.g. broadcast of SPaT, MAP and RTCM messages). The system operation requires and relies on functions and services provided by the core agency systems and certain external systems:

- SCMS for security
- Position corrections for RTCM messages
- Vendor systems for software updates
- Centralized system operational monitoring

Practical experience of several agencies showed that a reliable CI system requires system monitoring and expect to sustain through multiple iterations of software and configuration changes. Therefore, having these elements included on the diagram provides useful guidance of the expected evolution of the CI toward practical implementations. Especially if the system is expected to be a large scale, distributed system covering diverse intersection network.

I.2.2 Communications Architecture

The Communications View is shown on Figure 53. It depicts three layers common with the Services View (Figure 52). It also refers to several elements using the same names as in Figure 52. Its emphasis is to show different communication options for data exchanges between Field Network devices, Center Network systems and External Network systems.

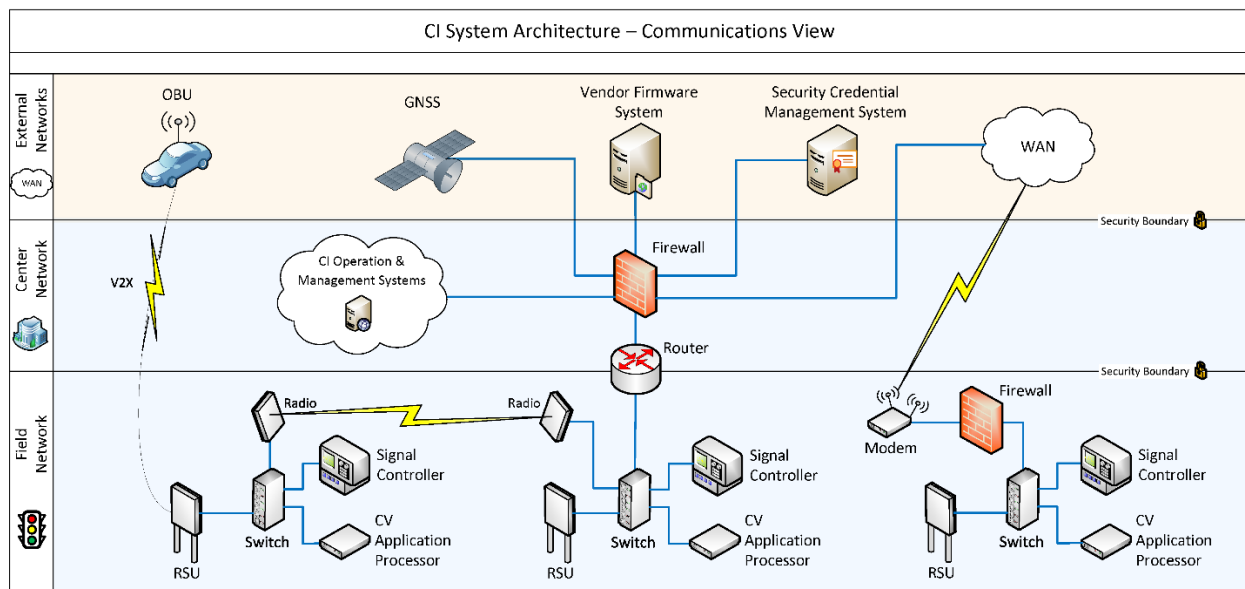


Figure 53. CI System Architecture – Communication View.

The Communication View shows three options to organize communication among field devices.

- The left group in the field network is a cluster of devices (i.e. an RSU, Edge Computer, Signal Controller, Network Switch) connected to the back-haul router using a point-to-point radio.
- The middle group has the same cluster of devices directly connected to the router via a hardwired link (e.g. fiber).
- The right group connects to the Center Network firewall using a cellular modem.

All these cases demonstrate connectivity options which allow the CI system to exchange data with the Center Network devices.

This diagram is useful to highlight the following dependencies:

- CI system requires RSUs to operate with security certificates. In order for RSUs to access SCMS certificates provided by the Security Credential Management System, network path and security rules have to be put in place within the Field and Center layers.
- A similar consideration required if an External Positional Reference System is utilized. Network and security rules have to be established to allow position correction messages to reach to RSUs.
- As highlight by network examples in the Field Network segment in Figure 53, a number of options is available to connect to the field devices ranging from fiber, wireless, cellular and other options as long as they can meet system requirements for network security and bandwidth for the CI system monitoring.
- Robust and secure communication between field devices and center network systems is essential to bring CV data from vehicles for processing and system monitoring. Certainly, data processing at the edge can significantly reduce the need to bandwidth, however, robust network still important for system monitoring and facilitating data collection and archiving for post-processing.
- Any network will work as long as it's secure (segmented), reliable and can handle large volumes of data if BSMs are forwarded for the CV Aggregation and Processing.
- Understanding of agency network is important for V2X deployment

During earlier CV pilot deployments, SPaT/MAP deployments were done with low bandwidth data and sometimes without connection to SCMS. This Communication View diagram highlights, that fully implemented CI system will require connection to SCMS and expect real-time system monitoring. Monitoring will be particularly important, as the system increases in the number of deployed nodes and system operational monitoring and security will involve large number of intersections.

1.3 Migration for Legacy Systems

There are numerous existing CV deployments across the United States, exhibiting various applications, and hardware capabilities. These deployments were established through previous pilot projects, research initiatives, and industry efforts such as "the SPaT Challenge" program. In this guidance, we anticipate that the majority of these sites will be upgraded to support the CI system described in this document. Following the publication of this document, new deployment sites will emerge specifically focused to support RLWV applications described in the CTI 4501.

A large number of currently deployed CV systems at intersections are already capable of broadcasting SPaT/MAP messages. These sites are equipped with RSUs connected to TSCs and may also include an ECLAs. Upgrading these sites could offer a straightforward path to implement RLWV requirements outlined in CTI 4501.

The table below summarizes the scope of implementation required for the CI. These changes which will be required for new sites and some of the changes may be applicable to the sites transitioning from existing intersection broadcasting SPaT/MAP. The list below assumes that any configuration changes are implemented as part of the corresponding component implementations.

Table 47. Upgrade Path from Existing SPaT/MAP Broadcast Sites to the CI System.

Component		Expected changes
Field Network		
1.	Install RSUs	<ul style="list-style-type: none"> RSUs are required to support NTCIP 1218 and CTI 4001 standards. It is recommended to use 3rd party certified RSUs (e.g., certified by OmniAir).
2.	Updates to traffic signal controller and cabinet	<ul style="list-style-type: none"> CI system will require TSCs supporting NTCIP 1202 (at least version 03B). Support of the Battelle TSCBM for generating SPaT messages has been deprecated. Some TSC can be updated using a software update. Some intersections may be required TSC hardware upgrades. When upgrading TSCs consider if those have been validated to support the RLVW application. Consider cabinet upgrades if the current cabinet is space or power limited, or cabinet monitoring is required.
3.	Use SCMS RSU certificates	<ul style="list-style-type: none"> CI system is required to use SCMS security for RSUs. RSUs need to be provisioned to receive security certificates from an authorized SCMS provider.
4.	Evaluate suitability of communication link to the TMC backoffice	<ul style="list-style-type: none"> Network link between field cabinets and backoffice is important for provisioning SCMS certificates to RSUs and monitoring CI status and performance. Network link needs to support reliable and secure connection between RSUs and SCMS, and allow for continuous system monitoring from the center office and may be fulfilled by several design approaches as depicted on Figure 53.
5.	Support broadcast of SPaT, MAP and RTCM messages.	<ul style="list-style-type: none"> RSU will support the interface with the TSC and be capable of broadcasting SPaT and MAP messages as specified in the CTI 4501. RSU must support for broadcasting RTCM messages as per J3258. RSUs may implement support for creating and signing RTCM messages from a message stream generated by the Positional Reference system including when RTCM may be created elsewhere and RSU will be required sign them and transmit over-the-air.
6.	MAP changes	<ul style="list-style-type: none"> MAP messages may need reevaluation and validation per J3238/2. GIS surveyor grade equipment may be required to achieve the required precision of GIS data used to create MAP messages. MAP messages will need periodic updates to reflect intersection changes due to road construction, lane changes, consistency with SPaT, and etc.
7.	System validation	<ul style="list-style-type: none"> Deployment of an operational CI is expected to require a formal testing and validation. SAE J3238 covers required test plans of SPaT and MAP messages at an intersection. Agency may need to self-certify system performance validation and perform appropriate cyber security validation as per (CTI 4501 Section 4.3.3.4.1). The agency will coordinate with the SCMS provider to define the scope of an acceptable validation acceptable to obtain SCMS certificates for each intersection.
8.	Validation reports	<ul style="list-style-type: none"> Every CI system in operations is expected to be registered with the SCMS Manager or an SCMS provider. Submitting the final validation report and subsequent periodic maintenance reports may be required in order to use SCMS production certificates.
Center segment		

Component	Expected changes
9. CI monitoring system	<ul style="list-style-type: none"> Deploying CI monitoring system is highly recommended. The monitoring system is expected to monitor operation of the Field segment components and report on system deviations, anomalies and outages.
10. Software upgradability	<ul style="list-style-type: none"> All components of the CI will require periodic software upgrade. Ensure that secure provisioning of software updates is available for all CI components.

I.4 Important Considerations for CI Deployers & Operators

This section provides a summary of best practices derived from lessons learned from the deployment of the CI. This section assumes that the reader is familiar with basic approaches for system integration of a connected vehicle system. Therefore, the items below only highlight certain topics that need to be considered early on during the CV system upgrade or deployment of the CI system.

- Network Data Link.** The CI will benefit from a reliable communication link from the TMC to RSUs to be used for SCMS certificate downloads, remote configuration, and system monitoring. Using a fiber-based network connections to each RSU is not required. A 3G/4G cellular link speed may be sufficient. Network link reliability and latency for accessing the field devices may be more important factors for operating and monitoring the field CI systems.
- Certified Products.** Use of certified or independently validated CV equipment will provide an extra quality cushion and reduce possible interoperability issues between RSUs and OBUs due to misinterpretation or changes of technical requirements. Independent validation of devices through programs established by such organizations as SCMS Manager or OmniAir can reduce post installation troubleshooting and shorten post-integration system testing and validation. Use of “open industry specifications” for TSC could simplify procurement and interoperability of CI systems.
- Network Management Expertise.** Network configuration is the essential expertise required from the IOO to deploy the CI. For example, an RSU installed in the field needs access to SCMS which is typically provided by an external cloud-based service. The RSU may utilize IPv6 data transport protocol which needs to be supported by the agency networking routers, switches, and firewalls, etc. Security considerations, e.g., IP address subnetting, VLAN isolation, RSU network access to SCMS and CORS networks, must be included in system planning and design and call for appropriate network expertise.
- Network Access & Security.** The CI system is expected to have access to services that may reside in different network domains or even outside of IOO network, e.g., SCMS, cloud data storage, CORS network, system monitoring, time synchronization. Access to these external services is often managed by a dedicated IT group which manages security, firewalls and access between networks. Establishing requirements and understanding constraints for data access to external resources can significantly accelerate system deployment.
- Time Synchronization.** Good time synchronization is required between RSUs and TSCs. Time synchronization is important because signal phase and timing information generated by TSCs, has to be interpreted and translated into SPaT messages which is often performed by RSUs. By virtue of having integrated positioning system (i.e., GPS), RSUs have access to the sub-millisecond accurate reference clock. TSCs are often synchronized to the source of AC power. In addition, TSCs are expected to be synchronized to a network or GPS reference clock using NTP or PTP protocols to be in sync with RSUs. The same applies to Auxiliary field equipment (i.e., ECLAs).
- SCMS Security.** The CI system requires that RSUs use SCMS security certificates to sign outgoing SPaT, MAP, and RTCM messages and verify signatures of incoming BSM messages. RSU signing certificates will typically last for 1-2 weeks. Therefore, each RSUs will be periodically reaching out to an SCMS provider and download new certificates and CRL. Ensuring that all

RSUs have up-to-date certificates can be an important service provided by the CI monitoring system.

- **On-going Technical Support.** RSU and TSC infrastructure requires capable technical and vendor support to support system software upgrades, integration, validation and evolution due to changing technology. These resources often engage external personnel who will need to be trained and given access to the appropriate system resources.
- **Use of ECLA.** ECLA as an auxiliary computing device residing in the traffic cabinet (in some cases called as V2X Hub or CV co-processor) could implement certain emerging services (MAP/TIM management, RTCM, TSP, AGP). ECLAs are especially suitable for an agency with a strong technical team. Without affecting TSC fundamental operation, ECLA can implement software required to bring and augment pieces which may be missing in specific vendor implementations for RSUs and TSCs. This allows the RSU to remain a vendor “neutral” device. However, as the CI system matures, it is expected in the future that functions of ECLAs may be absorbed into other devices and the need to deploy ECLAs may fade away.
- **System Monitoring and Performance Measurement Tools.** Good system monitoring and data analytics for the CI is strongly encouraged to detect field system outages and performance degradation. The monitoring system can support CI maintenance by detecting issues quicker and saving on field troubleshooting.
- **OBU Lifecycle.** Even though some IOOs will deploy their own OBUs in their fleet vehicles, it is safe to assume that OBUs will require a separate dedicated communication link (rather than via RSU) to gain network access to security certificates, OBU monitoring, software updates, etc. The agency OBU lifecycle is important and must be planned in parallel to CI deployment.
- **System Procurement.** Crucial factors to take into account when procuring components for a CI system include the need to encompass both hardware and software aspects. The procurement process must also factor in considerations for change management, component lifecycles, upgrades, and the availability of spare parts. Given continuous evolution of technical standards supporting the CI, software and firmware for various components can be provisioned contingent on maintaining device certification, passing compatibility, interoperability and acceptance testing and expectations for on-going bug fixes and software updates. The IOOs are encouraged to collaborate with adjacent agencies for best practices to ensure operational stability and interoperability among CI systems managed by different agencies.

I.4.1 Anticipated Changes in RLWV Environment

As technology continues to evolve, those responsible to implement the RLWV systems must anticipate and adapt to the forthcoming changes. These changes may manifest as refinements in system requirements, procurement prerequisites and expectations regarding operations and maintenance processes. This section offers an overview of the factors which can initiate updates and modifications to the CI system.

- **Changes in the underlying technical standards.** The CI outlined in the document is dependent on a range of technical standards specifically developed to ensure interoperability among CI systems deployed throughout the country. Section I.5 includes a list of core standards that are crucial to the functioning of the CI system. When new versions of these standards are published, it may necessitate subsequent updates to the system implementations, as well as the associated software and firmware components. Once these changes are implemented in the field devices, it becomes essential to reassess the interoperability of the CI system.
- **Firmware updates/release due to bug fixes and upgrade.** Various components of the CI will undergo periodic software updates. These updates will address bugs, improve security or can be used to add new features. These software updates need to be planned as part of on-going CI maintenance and must be deployed with care for system interoperability, operational stability and security.
- **Security certificate expiration, changes in trust chain, CRL updates.** The CI should expect ongoing changes in the security system. SCMS security certificates have finite expiration date and even the “long-lived” certificates will be periodically updated. SCMS providers will generate and distribute updated certificates including CRLs to the end devices such as RSUs, ECLAs,

TMC. The agency will need to monitor and ensure that anticipated certificate expiration and updates will not disrupt CI operation.

- **Road/lane geometry changes (temporary or permanent), restripe intersection.** The CI will need to handle various changes to the intersection lane geometry due to road restriping, construction or occasional lane closures. When these changes are anticipated, updated MAPs need to be prepared and distributed to affected RSUs. In other cases, CI monitoring system may detect discrepancy between intersection geometry described in MAP files and actual vehicle trajectories and alert operators for an action (e.g. temporarily disable RLVW application until discrepancy is resolved).

I.5 Useful References and Other Resources

I.5.1 Key Standards for System Deployment and Interoperability

There are several industry standards provide backbone requirements to ensure system interoperability for CTI. As the CV technology continues to evolve, the standards are expected to change and periodically be republished. It is recommended to monitor the following standards for version updates and update device procurement documents to ensure interoperability and support for the technology evolution. The table is concentrated on spotlighting standards affecting product and application levels. Those in-turn could reference additional underlying standards, which have been omitted for the sake of brevity.

To avoid duplications, Table 48 below omits listing specific versions of standards and refers the reader to consult the CTI 4501 Section 1.2.1.

Table 48. Backbone Standards

Identifier + Title	Summary	Impact
CTI 4501 Connected Intersections Implementation Guide	This document	Any changes to this standard can impact operational compliance and interoperability.
SAE J2735 V2X Communications Message Set Dictionary	SAE J2735 describes encoding of messages transmitted by the CI system.	Interoperability between RSUs and OBUs can be affected if incompatible versions of the SAE J2735 standard are implemented.
CTI 4001 Roadside Unit (RSU) Standard	This standard defines open industry requirements for an RSU.	Changes to the CTI 4001 may impact RSU conformance and procurement requirements.
NTCIP 1218 Object Definitions for Roadside Units	NTCIP 1218 defines an SNMP-based management interfaces with a roadside unit (RSU).	Changes to the NTCIP 1218 may impact RSU conformance and procurement requirements.
NTCIP 1202 Object Definitions for Actuated Signal Controllers (ASC) Interface	NTCIP 1202 defines an SNMP-based management interfaces with an Actuated Signal Controller Unit and establishes an interface between the TSC and a CV Roadside process such as an RSU.	Changes to the NTCIP 1202 may affect interface between TSC and RSU and may impact signal and timing data provided by a TSC to generate SPaT messages. CTI 4501 requires TSCs to supporting version 03B or later.

Other references:

- **Connected Intersection Guidance Document**
Summary of best practices for the deployment of a connected intersection.
Published by: Connected Vehicle Pool Fund Study

Link:

<https://engineering.virginia.edu/sites/default/files/common/Centers/CTS/CVPFS/projects/ConnectedIntersections/CI%20Guidance%20Document%20Version%202.0%20Final%20.pdf>

- **MAP Guidance Document**

Discusses best practices for creating MAP messages

Published by: Connected Vehicle Pool Fund Study

Link:

https://engineering.virginia.edu/sites/default/files/common/Centers/CTS/CVPFS/projects/MAP/MAP%20Guidance%20Document%20-%20Revision%202_06232023.pdf

- **Lessons Learned & Guidance Documents**

Checklist for a successful deployment of the V2I Hub platform that facilitates communication between connected vehicle hardware and traffic control systems

Published by: USDOT

Link: <https://www.itskrs.its.dot.gov/its/benecost.nsf/ID/4b08c9fd920173ff85258324005ad6a3>

- **Software Repositories**

USDOT tool for creating MAP messages using Satellite maps

Link: <https://webapp2.connectedvcs.com/isd/#>

- **USDOT software repository for the V2X Hub**

Link: <https://github.com/usdot-fhwa-OPS/V2X-Hub>

I.6 Considerations for CI On-going Operations and Maintenance

This section will discuss approaches for CI operations and maintenance in order to meet the system operating goals.

I.6.1 Expectations for Organizational Processes

Operation and maintenance of connected vehicle systems could be considered complementary to the operation of a traffic signal system. Deployers and operators may consider taking the following steps to ensure support of the CI in the agency operational processes:

- Incorporate CI system operation and maintenance (O&M) into existing organizational processes, for example, incorporating CI O&M into the traffic signal O&M.
- Implement on-going system monitoring and performance measurement for intersections supporting RLVW applications as part of central TMC function and system monitoring of traffic signals.
- Consider funding sources to support required system upgrades (software, firmware, security) which will ensure CI support of the up-to-date industry standards.
- Integrating CTI security with the agency-wide cyber security organizational practices.
- Consider participating in various industry forums (e.g. V2I Coalition, CTI standardization, Plugfests) to share and learn about industry best practices, validation and interoperability initiatives.

§