SURFACE VEHICLE RECOMMENDED PRACTICE

CTI 4501™

PropDft JAN2026

Issued Proposed Draft 2026-01-05

Superseding CTI 4501 v01.01

Connected Intersections Implementation Guide

RATIONALE

This Connected Intersection (CI) Implementation Guide is developed by engaging a broad community of stakeholders, including but not limited to infrastructure owners/operators, automobile original equipment manufacturers (OEMs) and their suppliers, roadside unit (RSU) manufacturers, and the end users of connected vehicle data and services. The guide is 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 Association (NEMA), and SAE International, contributed to ensuring balanced and effective stakeholder representation and adherence to standards development processes as Standards Development Organizations (SDOs).

This recommended practice is developed with the combined effort of stakeholders representing the industry at large including IOOs, OEMs, fleet and truck operators, safety advocacy groups, multimodal partners, and end users of data and services. Several associations including AASHTO, IEEE 1609 Working Group, ITE, NEMA, and SAE International are involved in ensuring balanced and effective stakeholder representation and adherence to a consensus-based standards development process.

Through collaboration with these stakeholders, this guide addresses ambiguities and gaps identified by early deployers, providing direction on how to generate consistent, interoperable messages for signalized intersections across the United States, including for automated transportation systems. Building on the USDOT-sponsored Cooperative Automated Transportation Clarifications for Consistent Implementations (CCIs) for Connected Signalized Intersections, this recommended practice focuses on harmonizing messages broadcasted by a connected signalized intersection.

TO PLACE A DOCUMENT ORDER:
Tel: 1-877-606-7323 (U.S. and Canada only)
Tel: 1-724-776-4970 (outside U.S. and Canada)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: http://www.sae.org

For more information on this standard, visit
https://www.sae.org/standards/content/PRODCODE/

TABLE OF CONTENTS

1. SCOPE

CTI 4501 defines the key capabilities and interfaces a connected signalized intersection must support to ensure interoperability with vehicles, including production vehicles, for state and local Infrastructure Owner Operators (IOOs). A connected intersection is defined as an infrastructure system that broadcasts SPaT, MAP, and optionally position correction data to vehicles.

This recommended practice 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 recommended practice 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 (RLVW) application. Although the focus of the recommended practice is on the RLVW application, requirements for other V2X applications related to connected intersections, including requirements for traffic signal controllers to generate the SPaT information, are also addressed assuming the connected intersection configuration and messages can support them and no significant effort was needed. The Needs to Requirements Traceability Matrix (NRTM) in 6.2.3 provides the guidance to IOOs for the procurement of a connected intersection.

Recognizing that some stakeholders require more in-depth guidance on specific aspects of connected intersections, Version 2 of the CI Implementation Guide has been reorganized into a main document and several companion subdocuments. The main document establishes the overarching framework – following a Systems Engineering Process (SEP) – and includes a Concept of Operations (ConOps) and an NRTM for a connected intersection; and the generic requirements, system design details, and a Requirements Traceability Matrix (RTM) for those generic requirements. These elements enable users to identify and procure connected intersection solutions that satisfy their specific needs.

The companion documents elaborate on specialized areas such as SPaT, MAP, security, and testing and validation, providing requirements and design details tailored for those subject areas. Figure 1 depicts the relationships among these subdocuments and other documents that support the implementation of a connected intersection. SAE J3258 addresses positioning corrections for all V2X applications in addition to connected intersections. SAE J3305 addresses Assured Green Period and utilizes SPaT messages, linking this document with CTI 4501/1. SAE J3238/1 links to both CTI 4501/1 and CTI 4501/4 by providing an example method for the testing and validation of SPaT information broadcasts. SAE J3238/2 similarly links CTI 4501/2 and CTI 4501/4 by providing an example method for linking the testing and validation of MAP broadcasts. By separating out these focused topics, this recommended practice more effectively supports IOOs, OEMs, suppliers, and application developers who need targeted information. Taken together, this recommended practice (hereafter called the implementation guide) and the companion documents ensure that connected intersection deployments align with national standards and support a high level of interoperability, ultimately facilitating safer and more efficient automated transportation systems.

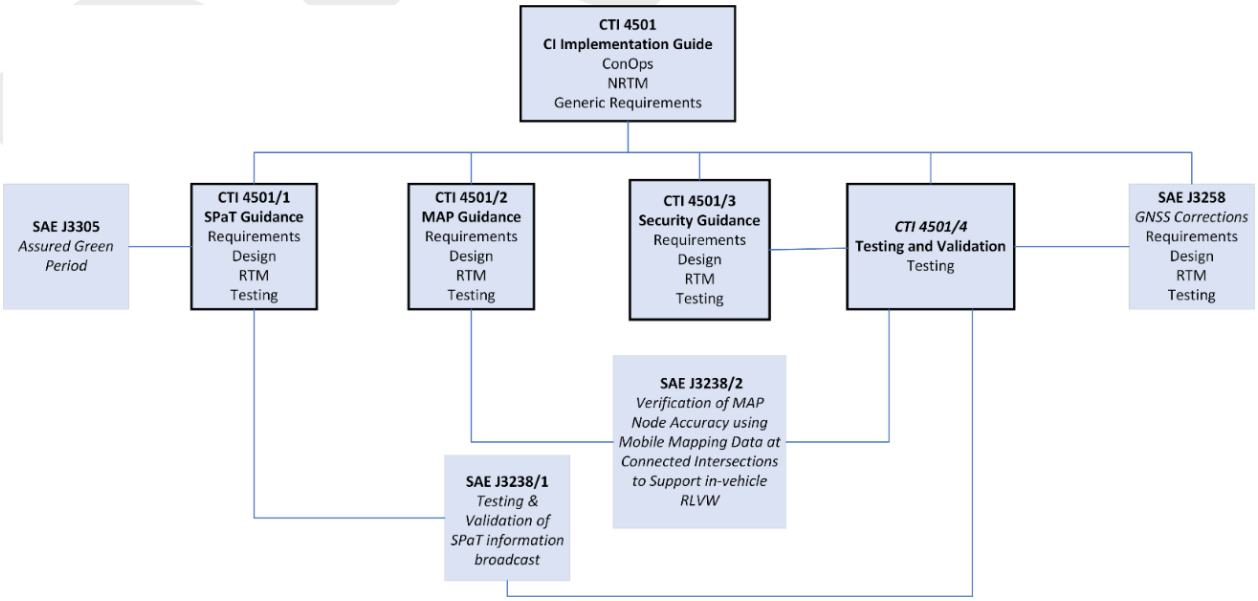


Figure 1 - Relationship with other documents

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this specification to the extent specified herein. Unless otherwise indicated, the latest issue of SAE International and other publications shall apply.

2.1.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 1-877-606-7323 (U.S. and Canada only) or 1-724-776-4970 (outside U.S. and Canada), www.sae.org.

SAE J2735 V2X Communications Message Set Dictionary

SAE J2945 Dedicated Short Range Communication (DSRC) Systems Engineering Process Guidance for SAE J2945/X Documents and Common Design Concepts™

SAE J3161 LTE Vehicle-to-Everything (LTE-V2X) Deployment Profiles and Radio Parameters for Single Radio Channel Multi-Service Coexistence

SAE J3161/1 Onboard System Requirements for LTE-V2X V2V Safety Communications

SAE J3161/2 LTE Vehicle-to-Everything (LTE-V2X) Deployment Profiles and Radio Parameters for PC5 Interface in 10 MHz Channel 180

SAE J3238/1 Testing and Validation of Broadcast SPaT from V2X Connected Intersections (CI) Supporting In-Vehicle Red Light Violation Warning (RLVW) Application

SAE J3258 V2X Infrastructure Support for GNSS Corrections

SAE J3268 Listing of Provider Service Identifiers and Associated Application Technical Reports

2.1.2 Connected Transportation Interoperability (CTI) Publications

CTI documents are jointly developed by American Association of State Highway and Transportation Officials, Institute of Transportation Engineers, National Electrical Manufacturers Association, and SAE International. Available at www.ite.org/technical-resources/standards/connected-intersections.

CTI 4001 Roadside Unit (RSU) Standard

CTI 4501/1 Connected Intersections (CI) Implementation Guide - SPaT Messages

CTI 4501/2 Connected Intersections (CI) Implementation Guide - MAP Messages

CTI 4501/3 Connected Intersections (CI) Implementation Guide - Security

CTI 4501/4 Connected Intersections (CI) Implementation Guide - Testing and Validation

CTI 4502 Connected Intersections Validation Report: Findings from the Connected Intersections (CI) Project Validation Phase

2.1.3 ETSI Publications

Copies of these documents are available online at www.etsi.org.

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]

2.1.4 IEEE Publications

Available from IEEE Operations Center, 445 and 501 Hoes Lane, Piscataway, NJ 08854-4141, Tel: 732-981-0060, www.ieee.org.

Please note that this report incorporates certain IEEE specifications by reference. ESSENTIAL IPRs (Intellectual Property Rights) have been declared to IEEE. All information statements and licensing declarations of ESSENTIAL IPRs received by IEEE are publicly available via the IEEE IPR Online Database found at https://standards.ieee.org/about/sasb/patcom/patents/.

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 Std 1609.2 IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages

IEEE Std 1609.2.1 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Certificate Management Interfaces for End Entities

IEEE Std 1609.3 IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services

2.1.5 Internet Publications

Available from several repositories on the World Wide Web, or by "anonymous" File Transfer Protocol (FTP) with several hosts. Browse or FTP to https://www.rfc-editor.org.

IETF RFC 4253 The Secure Shell (SSH) Transport Layer Protocol

IETF RFC 8446 The Transport Layer Security (TLS) Protocol

2.1.6 NIST Publications

Available from NIST, 100 Bureau Drive, Stop 1070, Gaithersburg, MD 20899-1070, Tel: 301-975-6478, www.nist.gov.

NIST FIPS 140-2 Security Requirements for Cryptographic Modules, https://doi.org/10.6028/NIST.FIPS.140-2

2.1.7 NTCIP Publications

Available from NTCIP Coordinator, National Electrical Manufacturers Association, 1812 N. Moore Street, Suite 2200, Arlington, VA 22209-3801, www.ntcip.org.

NTCIP 1202 National Transportation Communications for ITS Protocol Object Definitions for Actuated Signal Controllers (ASC) Interface

NTCIP 1218 National Transportation Communications for ITS Protocol Object Definitions for Roadside Units (RSUs)

2.1.8 RTCM Publications

Available from the Radio Technical Commission for Maritime Services, 1150 18th Street NW, Suite 910, Washington, DC 20036, Tel: +1 703-527-2000, www.rtcm.org/publications.

RTCM Standard 10410 RTCM 10410.1 Amendment 2, Standard for Networked Transport of RTCM via Internet Protocol (NTRIP) - An application-level protocol that supports streaming Global Navigation Satellite System (GNSS) data over the Internet

2.1.9 U.S. Department of Transportation, National Transportation Library

Available at https://github.com/usdot-fhwa-OPS/V2X-Hub/blob/develop/docs/V2I%20Hub%20Interface%20Control%20Document%20(ICD).pdf.

V2I Hub ICD Integrated Vehicle-to-Infrastructure Prototype (IVP), V2I Hub Interface Control Document (ICD) - Final Report.

2.2 Related Publications

The following publications are provided for information purposes only and are not a required part of this SAE Recommended Practice.

2.2.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 1-877-606-7323 (U.S. and Canada only) or 1-724-776-4970 (outside U.S. and Canada), www.sae.org.

SAE J2945/9 Vulnerable Road User Safety Message Minimum Performance Requirements

SAE J3287 V2X Misbehavior Reporting

SAE J3305 Assured Green Period to Support Red Light Violation Warning

SAE J3315 LTE-V2X Requirements and Deployment Profiles for Aftermarket V2X Devices

2.2.2 CAMP Publications

Available from Crash Avoidance Metrics Partners LLC, Tel: 248-848-9595, www.campllc.org/publications.

Red Light Violation Warning (RLVW) Application Vehicle System, Concept of Operations, Version 2.4, CAMP LLC, V2I-4 Consortium, 1/18/2021.

Red Light Violation Warning (RLVW) Application Vehicle System, High-Level System Requirements, Version 1.10, CAMP LLC, V2I-4 Consortium, 1/12/21.

2.2.3 Connected Vehicle Pooled Fund Study Publications

Copies of these documents are available online at https://engineering.virginia.edu/labs-groups/cvpfs.

CVPFS Connected Intersection Guidance Document

CVPFS CIMMS Systems Requirements, Connected Intersections Message Monitoring Systems Requirements and Prototype Development (CIMMS) Systems Requirements

CVPFS Guidance Document for MAP Message Preparation

Multi-Modal Intelligent Traffic Signal System (MMITSS) – Phase II: System Development, Deployment and Field Test

2.2.4 IEEE Publications

Available from IEEE Operations Center, 445 and 501 Hoes Lane, Piscataway, NJ 08854-4141, Tel: 732-981-0060, www.ieee.org.

IEEE Std 610.12	IEEE Standard Glossary of Software Engineering Terminology
IEEE Std 829	IEEE Std 829 IEEE Standard for Software and System Test Documentation
IEEE Std 1362	IEEE Guide for Information Technology System Definition - Concept of Operations (ConOps) Document

2.2.5 ISO Publications

Copies of these documents are available online at www.iso.org/store.

ISO/IEC/IEEE 24765	Systems and software engineering - Vocabulary
ISO 26262	Road vehicles - Functional safety
ISO/PAS 21448	Road vehicles - Safety of the intended functionality

2.2.6 National Academies Publications

Available at https://nap.nationalacademies.org/catalog/22097/signal-timing-manual-second-edition.

Signal Timing Manual	NCHRP Report 812 Signal Timing Manual

2.2.7 NEMA Publications

Available from National Electrical Manufacturers Association, 1812 N. Moore Street, Suite 2200, Arlington, VA 22209, Tel: 703-841-3200, www.makeitelectric.org.

NEMA TS 1	Traffic Control Systems
NEMA TS 2	Traffic Controller Assemblies with NTCIP Requirements
NEMA TS 40010	Connected Vehicle Infrastructure – Roadside Equipment

2.2.8 NTCIP Publications

Available from NTCIP Coordinator, National Electrical Manufacturers Association, 1812 N. Moore Street, Suite 2200, Arlington, VA 22209-3801, www.ntcip.org.

NTCIP 8002 Annex B1 National Transportation Communications for ITS Protocol Content Outline for NTCIP 1200-Series Documents (for Standards Engineering Process (SEP) Content)

NTCIP 9001 The NTCIP Guide

2.2.9 SCMS Manager Publications

Copies of these documents are available online at www.scmsmanager.org/publications.

End-entity Security Requirements, Design Guidance, and Validation Approach

2.2.10 U.S. Department of Transportation Publications, Tools, and Repositories

Available from U.S. Department of Transportation, 1200 New Jersey Avenue SE, Washington, DC 20590, Tel: 855-368-4200, www.transportation.gov.

Accelerated Vehicle-to-Infrastructure (V2I) Safety Applications System Requirements Document, FHWA-JPO-13-059, July 18, 2012, https://rosap.ntl.bts.gov/view/dot/26495/dot_26495_DS1.pdf.

ISD Message Creator, https://webappopen.connectedvcs.com/

Manual on Uniform Traffic Control Devices for Streets and Highways (MUTCD), https://mutcd.fhwa.dot.gov/

Systems Engineering for ITS Systems Engineering for ITS, https://ops.fhwa.dot.gov/seits/

V2I Hub Deployment Guide, https://www.itskrs.its.dot.gov/its/benecost.nsf/ID/4b08c9fd920173ff85258324005ad6a3

V2X Hub Software Repository, https://github.com/usdot-fhwa-OPS/V2X-Hub

2.2.11 U.S. Department of Transportation, National ITS Architecture

Available online at https://www.arc-it.net.

2.2.12 Other Publications

CCI Cooperative Automated Transportation Clarifications for Consistent Implementations (CCIs) To Ensure National Interoperability Connected Signalized Intersections

CIS Controls Guide CIS Controls™ Implementation Guide for Industrial Control Systems. Available at https://www.cisecurity.org/white-papers/cis-controls-implementation-guide-for-industrial-control-systems/.

Enabling Connected Intersections Concept Paper – Working Draft to Support Discussions of the IOO/OEM Forum SPaT/RLVW Group. Available at https://www.ite.org/ITEORG/assets/File/Standards/Enabling%20Connected%20Intersections%20-%20Concept%20Paper%20ver%202_8%20-%2002242020.pdf.

INCOSE Systems Engineering Handbook. Available at https://www.incose.org/.

3. DEFINITIONS

For the purposes of this document, the following definitions shall apply.

APPROACH: All lanes of traffic moving towards an intersection or a midblock location from one direction, including any adjacent parking lane(s). An approach is typically identified by its general flow, i.e., "the east-bound approach." In this document, an approach consists of one or more motor vehicle lanes of travel, as well as possible pedestrian lanes, parking lanes, barriers, and other types of lane objects some of which cross the path of the motor vehicle travel. Approach is also used in certain messages to specify where one or more lanes begin, regardless of whether the lane is ingress or egress. Source: SAE J2735

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): The UTC time denoting the end of a green signal indication for a movement. The AGET is set when the CI/TSC infrastructure determines when the through movement green interval will definitively 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 connected intersection in a through lane currently in a green signal state indication, the AGP is a fixed 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 connected intersection during a red signal state indication.

CI DATA: All data that is used in the CI system that has any effect on V2X messages. This includes data that is directly used in V2X messages, data that is transformed before being used in V2X messages, and data that is used in V2X messages only under particular conditions. It also includes configuration files that configure processes that produce data or messages; SCMS certificates and other credentials (including non-public certificates like the SCMS enrollment certificate); diagnostics and other self-monitoring information that is used to monitor and potentially alter the behavior of the system; and software and firmware updates.

CI DATA ENTITIES: Entities involved in creating and processing CI data. They may be inside or outside the CI.

CI DATA LOGICAL INTERFACE: The interface associated with any flow of CI data between two CI data entities where both entities "touch" the data and the receiver receives exactly the data/application bytes that the sender sent. If a flow goes A to B to C but B is a pure passthrough (and the system does not allow B to be anything other than a pure passthrough), then the logical interface is A to C, and there are no logical interfaces from A to B or B to C.

CI PERFORMANCE MONITORING SYSTEM (CPMS): A generic term for a central CI monitoring system.

COMPONENT: An element of the CI System. The element may be a device or a logical process.

CONNECTED INTERSECTION (CI): An infrastructure system that creates and broadcasts signal, phase, and timing (SPaT), mapping information, and position correction data to On-Board Units (OBUs) and Mobile Units (MUs).

CONNECTED VEHICLE: A vehicle equipped with devices enabling interoperable direct short-range broadcast communication to convey and receive safety- and mobility-enhancing messages.

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).

CRITICAL FAILURE: Any event that prevents the connected intersection from operating in Normal Mode.

EXTERNAL CONTROL LOCAL APPLICATION (ECLA): An application that asserts a higher-level control over the traffic signal controller.

FIRMWARE: Software tightly coupled to a specific piece of computing hardware. Typically used for control, configuration, and interface definition, and rarely interacted with directly by the user. It may be necessary for firmware to be updated from time to time, for example, to ensure the continued correct operation of the hardware or expose or enable new features.

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: NTCIP 9001

INTERFACE: A shared boundary across which information is passed. Source: IEEE Std 610.12

INTEROPERABILITY: The ability of two or more systems or components to exchange information and to use the information that has been exchanged. Source: IEEE Std 610.12

INTERSECTION or INTERSECTION BOX: Where a stop line, yield line, or crosswalk is designated on the roadway on the intersection approach, the area within the crosswalk and/or beyond the designated stop line or yield line shall be part of the intersection. If there are no stop lines, then the intersection box is defined by the extension of the curb lines. Refer to MUTCD for additional definitions of an intersection.

LONG TERM EVOLUTION–BASED VEHICLE-TO-EVERYTHING (LTE-V2X): Vehicle-to-everything (V2X) sidelink communications protocols specified by 3GPP (releases 14 and 15).

MAINTENANCE MODE: A mode of operation for a connected intersection, indicating an anomaly is preventing the connected intersection from operating in Normal Mode. This mode of operation also can be utilized for system updates.

MOBILE UNIT (MU): A device used to wirelessly communicate with other devices for safety and mobility purposes carried by a pedestrian, bicyclist, work zone worker, or other traveler. Source: CTI 4001

MOVEMENT: A term used to describe the user (e.g., vehicle or pedestrian) action taken at an intersection (e.g., vehicle turning movement or pedestrian crossing). Two different types of movements include those that have the right-of-way (protected/exclusive) and those that must yield (permitted/permissive), consistent with the rules of the road or the Uniform Vehicle Code. Source: Signal Timing Manual

NORMAL MODE: A mode of operation for a connected intersection, indicating the connected intersection operates with full capabilities, broadcasting SPaT, MAP, and RTCM messages, compliant to all mandatory requirements specified in this document.

ON-BOARD UNITS (OBU): A device used to wirelessly communicate with other devices for safety and mobility purposes installed in a vehicle as original equipment or as aftermarket equipment (sometimes referred to as an "aftermarket V2X device" [AVD]). Source: SAE J3315

PERMISSIVE MOVEMENT: 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.

PERMITTED MOVEMENT: A movement that is allowed to proceed if there are available gaps in the conflicting flow. Source: Signal Timing Manual

PREEMPTION: The transfer of the normal control of signals to a special signal control mode for the purpose of servicing railroad crossings, emergency vehicle passage, mass transit vehicle passage, and other special tasks, the control of which requires terminating normal traffic control to provide the higher priority needs of the special task. Source: NTCIP 1202

PROTECTED MOVEMENT: A permitted movement that has the right of way over other conflicting movements (including pedestrians) and is not required to yield to permissive movements. Traffic making a protected movement should be aware that conflicting traffic from other signal types (e.g., pedestrian signals) may need to clear the intersection before proceeding.

PROTECTED/PERMISSIVE MOVEMENT: A permitted movement at an intersection that, through the use of different signal indications, is protected (i.e., has the exclusive right-of-way over conflicting movements), during a defined portion of the signal operations and permissive (i.e., must yield the right-of-way to conflicting movements) during other portions of the signal operations.

PROVIDER SERVICE IDENTIFIER (PSID): An integer which identifies an application specification. Source: SAE J3268

RED LIGHT VIOLATION WARNING (RLVW) APPLICATION: An in-vehicle application intended to influence drivers approaching the intersection that are either unintentionally not stopping at red lights or would not pass the intersection before the red interval begins, both of which could lead to conflicts with cross-traffic. Source: RLVW Application Vehicle System, Concept of Operations

REVOCABLE LANE: A lane whose properties may be in effect or not. Lane properties in SAE J2735 are defined by the type of lane (e.g., a travel lane, a parking lane, a shoulder), the type of travelers that may use the lane (passenger vehicles, transit vehicles only, bicycles, pedestrians), and the direction of travel. A physical lane in the roadway may be defined by more than one lane identifier, each with a different set of lane properties, and a bit can be used to determine if that lane property is in effect or not. For example, a reversible lane may be defined by two lane identifiers, one for each direction of traffic, but only one (revocable) lane identifier is in effect.

RLVW DETECTION ZONE (RDZ): The area on a through movement lane that is used to detect connected vehicles for the RLVW operation.

ROADSIDE UNIT (RSU): A transportation infrastructure communications device located on the roadside that provides V2X connectivity between OBUs/MUs and other parts of the transportation infrastructure including traffic control devices, traffic management systems, and back-office systems. Note: Devices that are not part of the transportation infrastructure, such as cellular base stations or satellites, are not RSUs. Source: CTI 4001

ROBUSTNESS: Degree to which a system or component can function correctly in the presence of invalid inputs or stressful environmental conditions. Source: ISO/IEC/IEEE 24765

SIGNAL GROUP: A logical grouping of one or more traffic movements that are controlled by the same traffic signal indication (e.g., green, yellow, red). Each signal group typically governs the right-of-way for a specific set of vehicle or pedestrian movements at an intersection and is the basis for how signal timing is communicated in connected vehicle systems. Signal groups enable coordination between the SPaT and MAP messages by identifying which movements receive which signal indications. See MOVEMENT. Source: SAE J2735, section on DF_MovementState

SIGNAL GROUP ID: A numeric identifier assigned to a signal group within the Signal Phase and Timing (SPaT) message. It uniquely identifies which set of traffic movements is governed by a particular signal indication at a given intersection. This ID serves as the link between the SPaT message (which provides the signal state) and the MAP message (which defines the intersection's geometry and permitted movements). Source: SAE J2735, section on DF_MovementState

SIGNAL INDICATION: The illumination of a signal lens or equivalent device. Source: MUTCD

SIGNAL INTERVAL: The part of a signal cycle during which signal indications do not change. Source: MUTCD

SIGNAL TIMING DATA: For the purpose of this document, signal timing data for a CI is the movement state and information when a movement may end for each movement at an intersection.

SIGNAL TIMING STATUS: For the purpose of this document, signal timing status is the status of the signal controller, such as its mode of operation, and its failure state, if any.

SPaT INFORMATION: Signal phase and timing data, such as timing and movement state information for each movement through an intersection, which is sent from a traffic signal controller to another device. This document describes three methods to send SPaT information to RSUs.

STATUTORY SPEED LIMIT: A speed limit established by legislative action (such as Federal or State law) that typically is applicable for a particular class of highways with specified design, functional, jurisdictional, and/or location characteristics and that is not necessarily displayed on Speed Limit signs. Source: MUTCD

THROUGH MOVEMENT: A movement of a vehicle or pedestrian at an intersection where the direction of travel is unaltered by a left-, right-, or U-turn.

TIMEMARK: Used to relate a moment in UTC (Coordinated Universal Time)-based time (referenced from the top of the hour) when an event is predicted or expected to occur, such as a change in the signal indication). Timemarks are expressed as the number of 1/10th of seconds from the beginning (or top) of the hour. Refer to SAE J2735.

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.

TRAVEL LANE: The area of the roadway designated for the movement of a vehicle, pedestrian, bicycle, or designated user.

TSC INFRASTRUCTURE: The systems and components within the traffic cabinet that control the operations of the signal indications at a signalized intersection, including an external control local application (ECLA) that may assert a higher-level control over the traffic controller.

V2X: Vehicle-to-everything (V2X) communications are comprised of various connected devices including vehicles (V), infrastructure (I), and other devices (D). Subsets of V2X communications referenced in this document include vehicle to vehicle (V2V), vehicle-to-infrastructure (V2I), and infrastructure-to-vehicle (I2V). Source: SAE J3161

V2X VEHICLE: A vehicle equipped with devices enabling interoperable direct short-range broadcast communication using 3GPP-defined LTE-V2X Rel-14 PC5 mode to convey safety- and mobility-enhancing messages. The V2X vehicle defined and used in these documents does not include networked communications or commercial connected vehicle applications. Source: SAE J3161 and SAE J3161/1

VALIDATION: To provide objective evidence that the system, when in use, fulfills its business or mission objectives and stakeholder requirements, achieving its intended use in its intended operational environment. Source: ISO/IEC/IEEE 15288

VERIFICATION: To provide evidence that the system, the system elements, and the work products in the life cycle meet the specified requirements. Source: INCOSE Systems Engineering Handbook

VULNERABLE ROAD USER (VRU): A road user, who is not occupying a vehicle such as a passenger car, a motorcycle, a public transit vehicle, or a train. Pedestrians, cyclists, children, elderly, disabled people, and road workers are particularly vulnerable to serious injury or death when involved in a motor-vehicle-related collision. Source: SAE J2945/9

4. ABBREVIATIONS

Cited below are the abbreviations that are used in this report.

AASHTO	American Association of State Highway and Transportation Officials
AGET	Assured Green End Time
AGP	Assured Green Period
ARC-IT	Architecture Reference for Cooperative and Intelligent Transportation
AVD	Aftermarket V2X Device
CAT	Cooperative Automated Transportation Coalition
CCI	Clarifications for Consistent Implementations (document)
CI	Connected Intersection
ConOps	Concept of Operations
CORS	Continuously Operating Reference Station
CPMS	Connected Intersection Performance Monitoring System

CR	Channel Occupancy Ratio
CRL	Certificate Revocation List
CTI	Connected Transportation Interoperability
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
ICD	Interface Control Document
IEEE	Institute of Electrical and Electronics Engineers
IOO	Infrastructure Owner/Operator
ITE	Institute of Transportation Engineers
LTE-V2X	Long-Term Evolution Vehicle-to-Everything
MTBF	Mean Time Between Failures
MU	Mobile Units
MUTCD	Manual on Uniform Traffic Control Devices
NCHRP	National Cooperative Highway Research Program
NEMA	National Electrical Manufacturers Association
NRTM	Needs to Requirements Traceability Matrix
NTCIP	National Transportation Communications for ITS Protocol
NTP	Network Time Protocol
NTRIP	Network Transport of RTCM via Internet Protocol
O&M	Operations and Maintenance
OBU	On-Board Units
OEM	Original Equipment Manufacturers
OID	Object Identifier

PDB	Package Delay Budget
PPPP	ProSe per packet priority
ProSe	Proximity Services
PSID	Provider Service Identifier
PTP	Precise Time Protocol
RDZ	RLVW Detection Zone
RLVW	Red Light Violation Warning
RSRP	Reference Signal Receive Power
RSU	Roadside Unit
RTCM	Radio Technical Commission for Maritime Services
RTK	Real-Time Kinematic
RTM	Requirements Traceability Matrix
SAE	SAE International
SCMS	Security Credential Management System
SDO	Standards Development Organization
SEP	Systems Engineering Process
SPaT	Signal Phase and Timing
SPS	Semi-Persistent Scheduling
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
V2X	Vehicle-to-Everything
VRU	Vulnerable Road User
WAVE	Wireless Access in Vehicular Environments
WSM	WAVE Short Message

5. CONCEPT OF OPERATIONS

Section 5 defines the user needs that subsequent sections of CTI 4501 address. Accepted system engineering processes detail that requirements should be developed to satisfy 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 CTI 4501, this first stage entails identifying the various ways in which the IOOs may provide and OBUs/MUs 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 CTI 4501;

b. The key capabilities and interfaces for a connected intersection;

c. An understanding of the perspective of the developers of CTI 4501; and

d. A testing framework to verify conformance to CTI 4501.

Section 5 is intended for all readers and users of CTI 4501, including the following:

a. Transportation Managers: IOO personnel responsible for making decisions about operational strategies to implement and configure 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 are consistently and reliably provided by IOOs, and properly used by applications.

For the first five categories of readers, Section 5 is useful to understand what SPaT, MAP, and positioning data should be provided.

For the last three categories of readers, Section 5 provides a more thorough understanding as to why the more detailed requirements exist later in CTI 4501, and how SPaT and MAP data is derived.

5.1 Tutorial [Informative]

A ConOps describes a proposed system from the users' perspective. Typically, a ConOps is used to ensure that system developers understand the users' needs. Within the context of CTI 4501, the ConOps documents the intent of each feature that a connected intersection provides.

The term "Normative" is used to distinguish sections that are essential for the complete (and correct) understanding and implementation of this document. The term "Informative" is used to distinguish sections that are not essential but are there for informational purposes. It is possible for a section to be identified as Normative but have subsections that are identified as Informative. If a section is Normative, then all of its subsections are Normative unless identified otherwise.

The ConOps 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 the situation.

The ConOps then documents key aspects about the proposed system, including the following:

- Reference Functional Architecture: The reference functional architecture (view) defines the overall context of the connected intersection system and defines what components and interfaces are addressed by CTI 4501. The reference functional architecture is supplemented with one or more examples that describe how the reference functional architecture may be realized in an actual deployment.

- Needs: The needs identify and describe the various functions that users want components of the connected intersection to perform. These needs, also called features, are derived from the high-level user needs identified in the problem statement (see 5.2) but are refined and organized into a more manageable structure that forms the basis of the traceability tables contained in 6.2.

- Operational Scenarios: The operational scenarios allow a reader to understand the different parts of the proposed functions of a connected intersection 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 CTI 4501.

- Relationship to the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) [Informative]: This section describes how a CI implementation fits into the National ITS Architecture.

Section 6, Functional Requirements, uses the needs, also called features, identified in the analysis of the system to define the various requirements for a connected intersection. 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 satisfy 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 6 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 7.2, which defines how the requirement is fulfilled.

5.2 Current Situation and Problem Statement [Informative]

Connected Intersections are defined as an infrastructure system equipped to broadcast SPaT information, roadway geometric information, and position correction data to support safety applications on OBUs/MUs.

Connected intersections were initially deployed 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 broadcast SAE J2735 SPaT messages. 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. Connected intersections are now being broadly deployed around the US as part of several USDOT grant programs and a variety of independent initiatives undertaken by states and local jurisdictions.

Early deployments of connected intersections demonstrated that 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.

Figure 2 is a high-level architecture diagram of the RLVW application within the OBU in the context of a connected intersection.

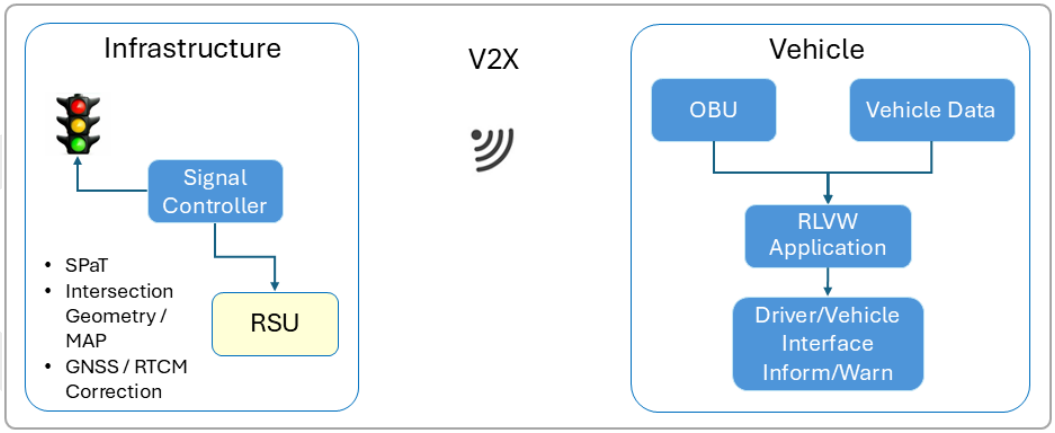


Figure 2 - Red light violation warning application context diagram

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 3 is a depiction of how IOOs use standards today, and the process issues IOOs encounter that could prevent national interoperability for connected intersections.

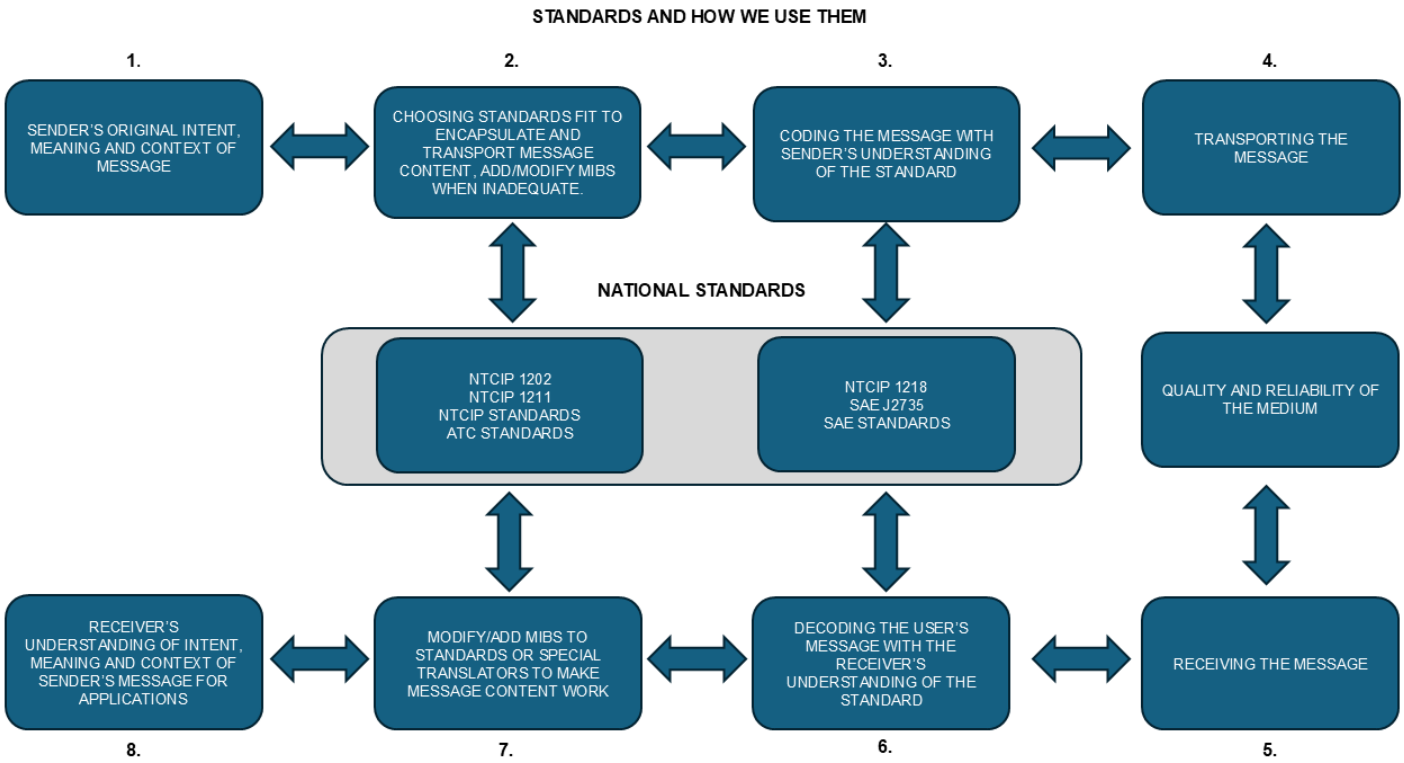


Figure 3 - How standards are used in a connected intersection

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. 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 another option.

Upon receiving the message, the receiver must decode the message and interpret 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, if the message is sent through 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 another 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 CTI 4501 is meant to address.

5.3 Reference Functional Architecture

5.3.1 Connected Intersection Architecture

This section presents an overview of what a complete CI "system" may look like for users, including the IOO that operates and maintains the infrastructure, and travelers through the connected intersection. The section describes the "actors" that participate in the connected intersection, including the producers and consumers of information, and are addressed by CTI 4501. Figure 4 is a graphical depiction (context diagram) of the physical architecture for the connected intersection.

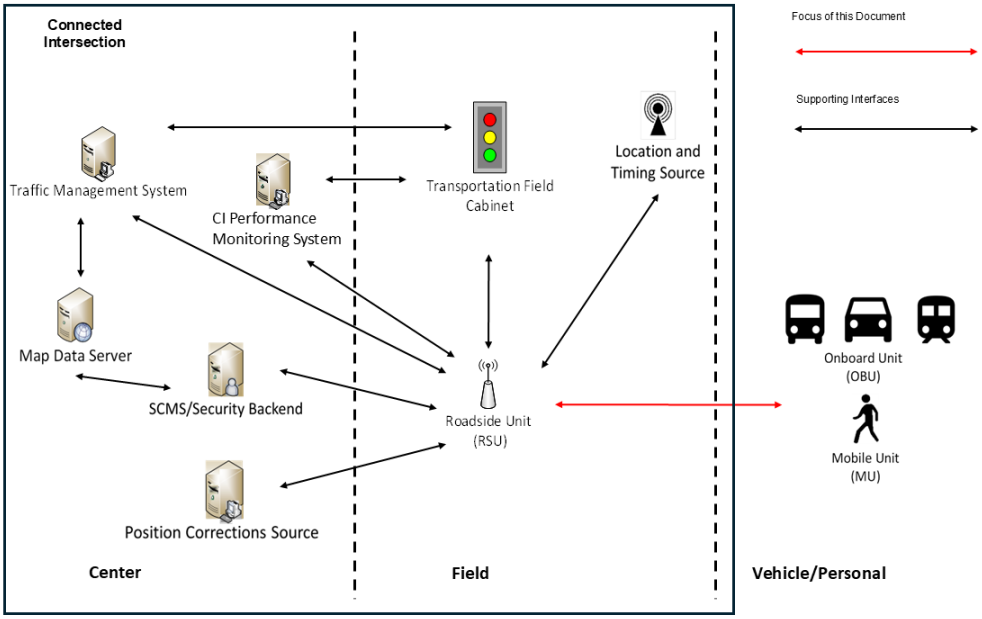


Figure 4 - Connected intersection

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: Intelligent infrastructure devices 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-V2X 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 traffic 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 traverse the intersection in a safe, orderly manner.

- Location and Timing Source: The source provides position and time information, which is typically from a Global Navigation Satellite System (GNSS).

- Position Corrections Source: The source represents the external source of land-based position corrections that augment satellite-provided (e.g., GNSS) positioning data. The Positioning Corrections source can be a single reference station or a Real-Time Kinematic (RTK) reference network. Intermediate processing between the source and RSU may also be present but is out of scope.

- On-Board Unit (OBU): Performs the data exchange between the infrastructure and a vehicle and is installed in a vehicle (includes an after-market device). An OBU contains 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 represent the interfaces that are addressed by CTI 4501, 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. Other interfaces may exist among the components outside a connected intersection, such as between the Security Credential Management System (SCMS)/Security Backend and the OBU/MU, but are not depicted in the diagram since those interfaces are not addressed by CTI 4501. Interfaces may also exist within the connected intersection itself based on what services are provided "inside" the connected intersection and where, but again, these interfaces are also not addressed by CTI 4501 except for requirements for the "TSC Infrastructure." The existence of these external ("outside") and internal ("inside") the connected intersection affects the security treatment in CTI 4501/3, but does not affect other requirements.

CTI 4501 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 5.6.1. However, needs for other SPaT-based and MAP-based safety applications, including needs for a traffic signal controller to generate the information for a SPaT message, are also included in CTI 4501.

5.3.2 TSC Infrastructure Architecture

Figures 5 and 6 are graphical depictions of the typical architecture inside the Transportation Field Cabinet for control of a signalized intersection. The connections shown are logical. Connections to external sensors are not shown because they are not two-way data connections. These architectures and components within the Transportation Field Cabinet are referred to as the TSC infrastructure. Figure 5 represents the most common architecture deployed at signalized intersections at the time this document is published.

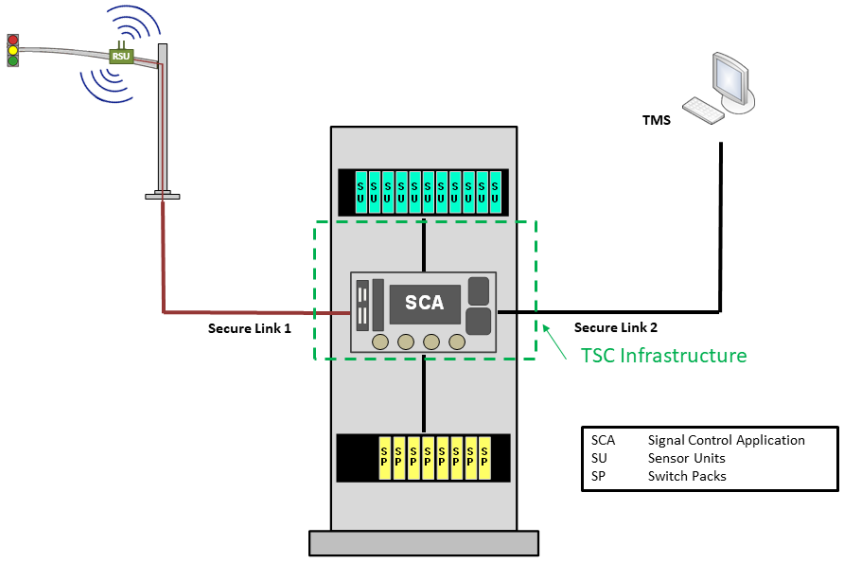


Figure 5 - Typical TSC infrastructure architecture

The elements involved are described below.

- Signal Control Application: Called the TSC Process in NTCIP 1202, represents the traditional processes providing control of a signalized intersection.
- Sensor Units: Called Detector Units in NTCIP 1202, 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 Pack: Called Load Switches in NTCIP 1202, 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 durations 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 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 provide the signal timing duration information in advance to the TSC 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 (refer to MMITSS and V2X Hub Software Repository).

Figure 6 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.

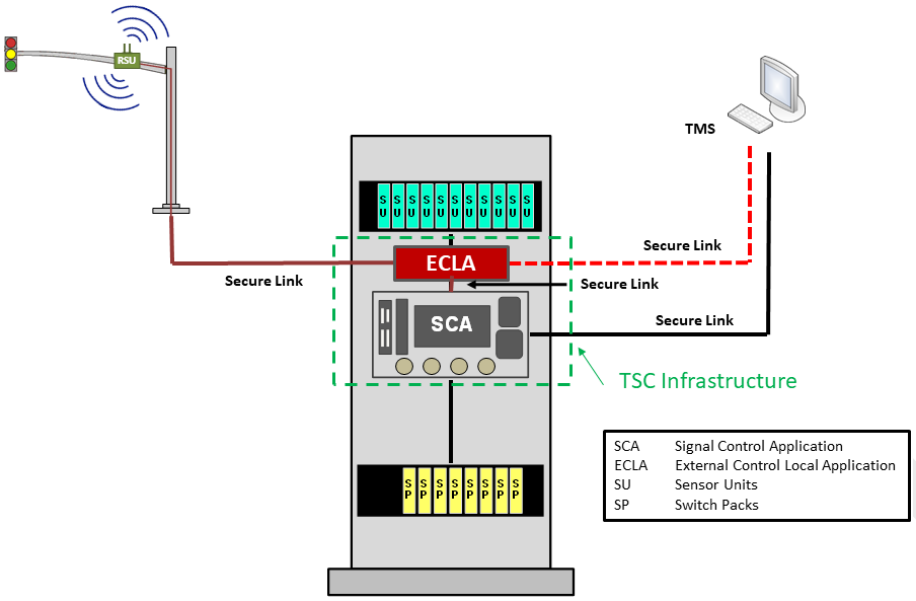


Figure 6 - TSC infrastructure (with ECLA) architecture

5.4 Needs

The needs for a connected intersection follow.

5.4.1 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 time so the application can properly process the data from the connected intersection 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.

5.4.2 Traffic Signal Controller Infrastructure Data

A 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. This section contains the needs for TSC infrastructure data.

5.4.2.1 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. Signal timing data for a connected intersection is the movement state, information on when the movement may end, and the signal group identifier for each movement at an intersection.

5.4.2.2 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. Signal timing status is the status of the TSC, such as its mode of operation, the validity of the data, or its failure state.

5.4.2.3 RLVW Support

This section identifies the TSC infrastructure user needs for the Red Light Violation Warning (RLVW) application.

5.4.2.3.1 Advance Notification of End of Green

A TSC Infrastructure needs to send an advance notification of the end of the green interval to a V2X vehicle approaching an intersection on a through movement. This notification is to have a high level of certainty of occurring. This enables the RLVW application on the connected vehicle to warn the driver if the vehicle is unlikely to be able to stop prior to entering the intersection or clear the intersection before the signal indication is red.

5.4.2.3.2 Clear Intersection Before Onset of Red Indication

A TSC Infrastructure needs to provide information to decrease the likelihood that a V2X vehicle approaching an intersection on a through movement will be in the intersection during a red signal indication. This has the potential to reduce collisions.

5.4.2.3.3 Receive Approaching Vehicle Information from an RSU

A TSC infrastructure needs to receive the position, speed, and heading for approaching V2X vehicles from an RSU. This enables the TSC infrastructure to provide additional support to the RLVW application.

5.4.3 Messages

This section identifies needs related to a connected intersection sending and receiving information to/from OBUs/MUs.

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

5.4.3.1 Message Performance Needs

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

5.4.3.1.1 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.

5.4.3.1.2 Robustness

A connected intersection needs to be robust. When subject to anomalous data and commands, the connected intersection and its components continue to function properly, can recover from these situations, and are not corrupted. These components may have different failure modes or 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.

5.4.3.1.3 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.

5.4.3.1.4 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 connected intersection where approach speeds are 20 miles per hour (mph) when compared to a connected intersection where the approach speeds are 50 mph.

5.4.3.1.5 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.

5.4.3.1.6 Quality Assurance

A connected intersection 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.

5.4.3.2 Generic Message Data Needs

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

5.4.3.2.1 Time Source

A connected intersection needs to use the same time reference and with sufficient precision and accuracy as OBUs/MUs so CV 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.

5.4.3.2.2 Message Revision

A connected intersection needs to indicate if the data provided on a specific topic (other than the timestamp) has changed since the last transmitted message. This allows the receiving application to make a determination as to whether it should process the data.

5.4.3.2.3 Timestamp

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

5.4.3.3 Signal Timing Data Needs

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

5.4.3.3.1 Intersection Identification

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

5.4.3.3.2 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.

5.4.3.3.3 Current Movement State

A connected intersection needs to provide information about the current state of each movement, including 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, stop and remain, or stop and may proceed with caution with possible conflicting traffic.

5.4.3.3.4 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 a movement through an intersection will be allowed and any restrictions for the next signal interval. 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.

5.4.3.3.5 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: 5.6.2.1 - Rest in Green.

5.4.3.3.6 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.

5.4.3.3.7 Enabled Lanes

A connected intersection needs to provide information about which lanes and lane attributes are currently active (enabled) so an application can determine what attributes are currently in effect 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.

5.4.3.3.8 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 traffic 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.

5.4.3.4 Roadway Geometry Data Needs

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

5.4.3.4.1 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.

5.4.3.4.2 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.

5.4.3.4.3 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.

5.4.3.4.4 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.

5.4.3.4.5 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.

5.4.3.4.6 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 active.

5.4.3.4.7 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. Enough accuracy is desired so the vehicle can determine which lane it is in, since different lanes may be controlled by different signal indications being in different states. Inaccurate data reduces the effectiveness of the applications that use the data.

5.4.3.4.8 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 in agreement. If an entity changes the design geometry environment, it may necessitate a change in the signal timing data.

5.4.3.5 Positioning Data Needs

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

5.4.3.5.1 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.

5.4.3.5.2 Real-Time Kinematic Corrections

RSUs at connected intersections need to broadcast the appropriate Real-Time Kinematic (RTK) corrections messages in accordance to the methods described in SAE J3258, 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.

5.4.3.6 Vehicle Data Needs

This section identifies needs about connected vehicles around a connected intersection.

5.4.3.6.1 Vehicle Position and Kinematics

A connected intersection needs to know about the position and kinematics (velocity, position, acceleration) of vehicles approaching the connected intersection so it can determine the vehicle demand at the intersection and has the ability to safely and efficiently service that demand.

5.4.4 Security

This section identifies security needs for a connected intersection. In this section, each security user need is traceable to one or more functional user needs. This ensures that security features support the functional operations of the system. The description of each security user need includes inline the identification of the functional user need(s) from which it is required.

NOTE: The identifiers (section numbers) for the security user needs in this document are NOT backward compatible with the identifiers in CTI 4501 v01.

5.4.4.1 Data Trustworthiness

This section identifies security needs associated with data trustworthiness.

5.4.4.1.1 Data Trustworthiness: Sources

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 correctly reflects near-real time CI operating conditions, allowing applications and users to react appropriately.

Derived from: 5.4.1, 5.4.3.1.6; also, a generalization of the individual trustworthiness goals in 5.4.4.1.3.

See also: 5.4.4.3.1, 5.4.4.3.2.

5.4.4.1.2 Data Trustworthiness: 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 messages created using that transformed data correctly reflect near-real time operating conditions, allowing applications and users to react appropriately.

Derived from: 5.4.1, 5.4.3.1.6; also, a generalization of the individual trustworthiness goals in 5.4.4.1.3.

See also: 5.4.4.3.3, 5.4.4.3.4.

NOTE: Although the other functional user needs do not directly identify platforms that modify or transform data, the architecture does identify that these platforms will exist, allowing the derivation of this user need.

5.4.4.1.3 Data Trustworthiness: Specific

This section contains specific data trustworthiness user needs derived directly from functional user needs.

5.4.4.1.3.1 Signal Timing Data Trustworthiness

The signal timing data provided by the TSC infrastructure to the RSU needs to be trustworthy so that the RSU can create trustworthy SPaT messages.

Derived from: 5.4.2.1.

5.4.4.1.3.2 Signal Timing Status Trustworthiness

The signal timing status provided by the TSC infrastructure to the RSU needs to be trustworthy so that the RSU can create trustworthy SPaT messages.

Derived from: 5.4.2.1.

5.4.4.1.3.3 Approaching Vehicle Information Trustworthiness: RSU

The information about approaching V2X vehicles received at the RSU needs to be trustworthy so that the RSU can provide trustworthy information to the TSC infrastructure.

Derived from: 5.4.2.3.3.

5.4.4.1.3.4 Approaching Vehicle Information Trustworthiness: TSC

The information about approaching V2X vehicles received by the TSC infrastructure from the RSU needs to be trustworthy so the TSC infrastructure can safely use the information to support the RLVW application.

Derived from: 5.4.2.3.3.

5.4.4.1.3.5 Time Source Trustworthiness

A connected intersection needs mechanisms to ensure that it cannot be maliciously manipulated into using a time source that is not synchronized with the time source used by receiving applications, so that the receiving application can safely use signal timing information.

Derived from: 5.4.3.2.1.

5.4.4.1.3.6 Message Revision Trustworthiness

A connected intersection needs mechanisms to ensure that information about whether a message is new is trustworthy so that the receiving application can safely use that information.

Derived from: 5.4.3.2.2.

5.4.4.1.3.7 Timestamp Trustworthiness

A connected intersection needs mechanisms to ensure that information about when data is generated by the infrastructure is trustworthy so that the receiving application can safely use that information.

Derived from: 5.4.3.2.3.

5.4.4.1.3.8 Intersection Identifier Trustworthiness

A connected intersection needs mechanisms to ensure that intersection identification information is trustworthy so that the receiving application can safely use that information.

Derived from: 5.4.3.3.1.

5.4.4.1.3.9 Intersection Status Trustworthiness

A connected intersection needs mechanisms to ensure that information about the intersection status is trustworthy so that the receiving application can safely use that information.

Derived from: 5.4.3.3.2.

5.4.4.1.3.10 Current Movement State Trustworthiness

A connected intersection needs mechanisms to ensure that information about the current movement state is trustworthy so that the receiving application can safely use that information.

Derived from: 5.4.3.3.3.

5.4.4.1.3.11 Next Movement State Trustworthiness

A connected intersection needs mechanisms to ensure that information about the next movement state is trustworthy so that the receiving application can safely use that information.

Derived from: 5.4.3.3.4.

5.4.4.1.3.12 Time Change Details Trustworthiness

A connected intersection needs mechanisms to ensure that information about the state change timing is trustworthy so that the receiving application can safely use that information.

Derived from: 5.4.3.3.5.

5.4.4.1.3.13 Next Allowed Movement Time Trustworthiness

A connected intersection needs mechanisms to ensure that information about the next allowed movement time is trustworthy so that the receiving application can safely use that information.

Derived from: 5.4.3.3.6.

5.4.4.1.3.14 Enabled Lanes Trustworthiness

A connected intersection needs mechanisms to ensure that information about enabled lanes is trustworthy so that the receiving application can safely use that information.

Derived from: 5.4.3.3.7.

5.4.4.1.3.15 Signal Timing and Roadway Indications Synchronization Trustworthiness: Robustness

A connected intersection needs mechanisms to ensure that synchronization between signal timing data and actual signal changes EITHER is correct in the presence of malicious actors so that it can safely be sent and used by the receiving application that can safely use that information, OR is known to be incorrect if it is incorrect, allowing the system to react so that a receiving application does not use incorrect information.

Derived from: 5.4.3.3.8.

5.4.4.1.3.16 Signal Timing and Roadway Indications Synchronization Trustworthiness: Correct Information

A connected intersection needs mechanisms to ensure that information within the system about synchronization between signal timing data and actual signal changes is correct, so that the system responds correctly to the situation and does not respond based on false information.

Derived from: 5.4.3.3.8.

5.4.4.1.3.17 Intersection Geometry Trustworthiness

A connected intersection needs mechanisms to ensure that information about intersection geometry is trustworthy so that the receiving application can safely use that information.

Derived from: 5.4.3.4.1.

5.4.4.1.3.18 Lane Attributes Trustworthiness

A connected intersection needs mechanisms to ensure that information about the allowed use of each lane is trustworthy so that the receiving application can safely use that information.

Derived from: 5.4.3.4.2.

5.4.4.1.3.19 Allowed Maneuvers Trustworthiness

A connected intersection needs mechanisms to ensure that information about allowed maneuvers of lanes is trustworthy so that the receiving application can safely use that information.

Derived from: 5.4.3.4.3.

5.4.4.1.3.20 Connections Between Lanes Trustworthiness

A connected intersection needs mechanisms to ensure that information about connections between lanes is trustworthy so that the receiving application can safely use that information.

Derived from: 5.4.3.4.4.

5.4.4.1.3.21 Approach Speed Limits Trustworthiness

A connected intersection needs mechanisms to ensure that information about approach speed limits is trustworthy so that the receiving application can safely use that information.

Derived from: 5.4.3.4.5.

5.4.4.1.3.22 Revocable Lanes Trustworthiness

A connected intersection needs mechanisms to ensure that information about revocable lanes is trustworthy so that the receiving application can safely use that information.

Derived from: 5.4.3.4.6.

5.4.4.1.3.23 Road Geometry Accuracy Trustworthiness

A connected intersection needs mechanisms to ensure that information about road geometry, once measured to the appropriate accuracy, cannot be changed unless the road geometry also changes, so that the receiving application can safely use that information.

Derived from: 5.4.3.4.7.

5.4.4.1.3.24 Signal Timing and Roadway Geometry Synchronization Trustworthiness

A connected intersection needs to have mechanisms to ensure that a malicious actor cannot cause it to send roadway geometry that is not reflective of the current operating state.

In particular, if the operating state changes, the connected intersection needs to have mechanisms to ensure that the malicious actor cannot prevent the geometry information from also changing, and cannot cause the connected intersection to send a previous message that is no longer accurate in a way that would lead the receiver to make use of that no longer accurate information.

This is necessary so that the receiving application can safely use that information.

Derived from: 5.4.3.4.8.

5.4.4.1.3.25 RTK Corrections Message Trustworthiness

A connected intersection needs mechanisms to ensure that RTK corrections messages sent via RTCM protocol defined in SAE J3258 are trustworthy so that the receiving application can safely use that information.

Derived from: 5.4.3.5.2.

5.4.4.2 Security Needs: Data in Transit

This section identifies security needs associated with integrity of data in transit.

5.4.4.2.1 Integrity of Data Passing Across Interfaces within the CI

A connected intersection needs to ensure that if CI data is corrupted or changed as it passes across interfaces within the connected intersection, those illegitimate changes can be detected within the connected intersection or by the receiving application, so that the receiving application can identify and discard incorrect messages.

Derived from: 5.4.1.

5.4.4.2.2 Assurance of Trustworthiness of Messages Sent from CI

A connected intersection needs to provide assurance to a receiving application that CI messages are created via a trustworthy process, so that the receiving application can safely use that data or messages based on that data.

Derived from: a generalization of the individual integrity goals in 5.4.4.1.3.

5.4.4.2.3 Integrity of Messages Sent from CI

A connected intersection needs to ensure that if CI messages are corrupted or changed after creation and transmission by the connected intersection, those illegitimate changes can be detected by the receiving application, so that the receiving application can identify and discard incorrect messages.

Derived from: a generalization of the individual integrity goals in 5.4.4.1.3.

5.4.4.3 Security Needs: Resilience

This section identifies security needs associated with the resilience needs of the CI system.

5.4.4.3.1 Data Sources: Resilience

A connected intersection needs to be able to minimize the impact on receiving applications if data sources are not behaving in a trustworthy way, so that attacks and other failures of trustworthiness do not have a significant impact on those receiving applications.

Derived from: 5.4.1, 5.4.3.1.2, 5.4.3.1.6, 5.4.4.1.1.

5.4.4.3.2 Data Sources: Recovery

A connected intersection needs to be able to return to correct operations if it is detected that data sources are not behaving in a trustworthy way, so that attacks and other failures of trustworthiness do not have a persistent impact on receiving applications.

Derived from: 5.4.1, 5.4.3.1.2, 5.4.3.1.6, 5.4.4.1.1.

5.4.4.3.3 Data Processing: Resilience

A connected intersection needs to be able to minimize the impact on receiving applications if data processing or modification processes, other than data sources, are not behaving in a trustworthy way, so that attacks and other failures of trustworthiness do not have a significant impact on those receiving applications.

Derived from: 5.4.1, 5.4.3.1.2, 5.4.3.1.6, 5.4.4.1.2.

5.4.4.3.4 Data Processing: Recovery

A connected intersection needs to be able to return to correct operations if it is detected that data processing or modification processes, other than data sources, are not behaving in a trustworthy way, so that attacks and other failures of trustworthiness do not have a persistent impact on those receiving applications.

Derived from: 5.4.1, 5.4.3.1.2, 5.4.3.1.6, 5.4.4.1.2.

5.4.4.4 Diagnostics and Reporting Security

This section identifies security user needs associated with the diagnostics system.

5.4.4.4.1 Diagnostics for Security Issues

A connected intersection's diagnostic system needs to include functionality to detect and remediate appropriately defined security issues so that the system is not vulnerable to attacks that are well-known and significant.

Derived from: 5.4.5.4.

5.4.4.4.2 Diagnostics for Incorrect Operations

A connected intersection’s diagnostic system needs to include functionality to determine whether the messages being sent by the connected intersection are incorrect so that the system can react and prevent receiving applications from using incorrect messages.

Derived from: 5.4.5.4.

5.4.4.4.3 Confidential Information within Diagnostics Systems

A connected intersection’s diagnostic system needs to prevent bad actors from accessing confidential diagnostic data to protect against data being accessed by parties that might make bad use of it.

Derived from: 5.4.5.4.

5.4.4.4.4 Correct Information within Diagnostics System

A connected intersection’s diagnostic system needs to prevent bad actors from modifying diagnostic data and providing incorrect information to the system administrators so that the system administrators have correct information and can make correct decisions about the operation of the system.

Derived from: 5.4.5.4.

5.4.4.4.5 Confidential Information within Performance Monitoring Systems

A connected intersection’s performance monitoring system (CPMS) needs to prevent bad actors from accessing confidential performance data to protect against data being accessed by parties that might make bad use of it.

Derived from: 5.4.5.5.

5.4.4.4.6 Correct Information within Performance Monitoring Systems

A CPMS needs to prevent bad actors from modifying performance data and providing incorrect information to the system administrators so that the system administrators have correct information and can make correct decisions about the operation of the system.

Derived from: 5.4.5.5.

5.4.4.5 Operations and Life Cycle

This section identifies security needs associated with the operations and life cycle user needs of the connected intersection.

5.4.4.5.1 Security Interoperability

A connected intersection's communications security mechanisms need to maintain interoperability with other CI systems within North America over an extended period of time so that receiving applications can use identical mechanisms (as near as possible) to trust all appropriately trustworthy connected intersections.

Derived from: 5.4.5.1.

5.4.4.5.2 Life Cycle Security Needs

This section identifies life cycle security needs for a connected intersection.

5.4.4.5.2.1 Security for Initial Installation

A connected intersection's life cycle processes for initial installation need to be appropriately secure so that receiving applications can have trust in received messages.

Derived from: 5.4.5.2.

5.4.4.5.2.2 Security for Security Certificate Provisioning

A connected intersection's life cycle processes for security certificate provisioning need to be appropriately secure so that receiving applications can have trust in received messages.

Derived from: 5.4.5.2.

5.4.4.5.2.3 Security for Normal Operations with System Monitoring and Anomaly Detection

A connected intersection's life cycle processes for normal operations with system monitoring and anomaly detection need to be appropriately secure so that receiving applications can have trust in received messages.

Derived from: 5.4.5.2.

5.4.4.5.2.4 Security for Maintenance/Degraded Operations

A connected intersection's life cycle processes for maintenance/degraded operations need to be appropriately secure so that receiving applications can have trust in received messages.

Derived from: 5.4.5.2.

5.4.4.5.2.5 Security for System Outages

A connected intersection's life cycle processes for system outages need to be appropriately secure so that receiving applications can have trust in received messages.

Derived from: 5.4.5.2.

5.4.4.5.2.6 Security for Equipment Upgrades/Swap-Out

A connected intersection's life cycle processes for equipment upgrades/swap-out need to be appropriately secure so that receiving applications can have trust in received messages.

Derived from: 5.4.5.2.

5.4.4.5.2.7 Security for Software/Firmware Updates

A connected intersection's life cycle processes for software/firmware updates need to be appropriately secure so that receiving applications can have trust in received messages.

Derived from: 5.4.5.2.

See also: 6.3.5.3.5.

5.4.4.5.2.8 Security for System Revalidation Following Recovery or Changes

A connected intersection's life cycle processes for system revalidation following recovery or changes need to be appropriately secure so that receiving applications can have trust in received messages.

Derived from: 5.4.5.2.

5.4.4.5.2.9 Security for Equipment Removal/Decommissioning

A connected intersection's life cycle processes for equipment removal/decommissioning need to be appropriately secure so that receiving applications can have trust in received messages.

Derived from: 5.4.5.2.

5.4.4.5.3 Maintenance Security Needs

A connected intersection's security mechanisms need to be capable of being managed as part of the normal Operations and Maintenance (O&M) infrastructure supported by the IOO (possibly with additional training/tools and with the addition of a credential supplier as an additional supplier to the IOO).

Derived from: 5.4.5.3.

5.4.4.5.4 System Upgradeability Security Needs

This section identifies system upgradeability security needs for a connected intersection.

5.4.4.5.4.1 Upgrade System: Correct Operation

A connected intersection's upgradeability, provisioning, and update system needs to prevent malicious installation of incorrect updates.

Derived from: 5.4.5.6.

5.4.4.5.4.2 Upgrade System: Correct Status

A connected intersection's upgradeability, provisioning, and update system needs to prevent malicious modification of status data to make it appear that the connected intersection is in a different update state than it actually is.

Derived from: 5.4.5.6.

5.4.4.6 Security Performance Needs

This section identifies security performance needs for a connected intersection.

5.4.4.6.1 Security Performance: Size

A connected intersection needs to use security mechanisms that do not have excessive message size overhead per the intent of the user need "concise messages."

Derived from: 5.4.3.1.3.

5.4.4.6.2 Security Performance: Latency

A connected intersection needs to use security mechanisms that do not create processing latency per the intent of the user need "Advanced Notification."

Derived from: 5.4.3.1.5.

5.4.4.7 Privacy Needs

A connected intersection needs to ensure that privacy-sensitive information is identified and protected against unauthorized disclosure.

5.4.5 Operations and Maintenance Needs

This section identifies O&M needs for a connected intersection.

5.4.5.1 Interoperability and Longevity

A connected intersection needs to reliably (i.e., over an extended period of time) operate consistently with other connected intersections so that OBUs/MUs will have a consistent experience across all connected intersections that they interact with. A connected intersection has to comply with all mandatory requirements in CTI 4501 over an extended period of time. This need also expresses an idea that CI deployments complying to CTI 4501 will achieve consistency and interoperability among different CI deployments. Furthermore, operating in compliance over an extended period of time, connected intersections will achieve system availability, promote ubiquity, robustness, implementation uniformity across different end-user interfaces, and high user acceptance.

5.4.5.2 Life Cycle

A connected intersection life cycle 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.

5.4.5.3 Maintenance

A connected intersection needs to be maintained and operated as part of the normal O&M infrastructure supported by the IOO. The connected intersection should be managed at the level of skills and capabilities of existing resources (with additional training, appropriate tools, etc.). Also, the connected intersection 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 connected intersection to meet application safety, system security, and operational objectives.

The IOO should recognize that a connected intersection may have special and unique testing/QA and performance considerations that may require special approaches compared to traditional ITS maintenance and cycle.

5.4.5.4 System Diagnostic Interface

A connected intersection must support self-diagnostic capabilities to avoid sending wrong, inconsistent, or incomplete information. Therefore, the connected intersection needs adequate diagnostic capabilities to detect any critical failures (i.e., anything that prevents the connected intersection from operating in Normal operational mode [defined in requirements]), measure system performance indicators (e.g., time tolerance, message flow, message accuracy), and report them through a monitoring and management interface.

This need also applies to each system component so it can detect outages in its operational condition and attempt to recover back to the normal operation. The component outages and critical failures have to be reported to the CPMS.

5.4.5.5 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.

5.4.5.6 System Upgradeability

A connected intersection needs to support upgradeability, provisioning, and updates to support expected system life cycle 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 (vehicles, mobile units, etc.).

5.4.5.7 System Recovery

A connected intersection needs to withstand interruptions and outages of its individual components "gracefully." If component self-recovery from a critical failure is not possible within an expected time, the connected intersection must alter its system state into a degraded state and notify the CPMS of the change. Once the outage of a system and/or its components is resolved, the system has to return into a normal operating state without operator intervention.

5.4.5.8 Self-Correcting Operation

A connected intersection needs to detect and notify its CPMS of any incorrect information that may be sent.

5.5 Operational Policies and Constraints

The following operational policies and constraints apply to the use of CTI 4501:

a. The operation and maintenance of the connected intersection is governed by the regulatory guidelines or policies for the IOO that may include USDOT's and the relevant states' Manual on Uniform Traffic Control Devices (MUTCD), and state and local ordinances, policies, and procedures.

b. The operation and maintenance of the connected 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 Functional Safety (FuSa) and Safety Of The Intended Functionality (SOTIF) requirements, for example, those specified in Federal Motor Vehicles Safety Standards, ISO 26262, ISO/PAS 21448, 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.

5.6 Operational Scenarios [Informative]

According to IEEE Std 1362,

> 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 Std 1362]

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 (as this is the appropriate environment in which to consider red light violations that are due to driver inattention at moderate to high speeds). The operational scenarios provided:

- Allows a reader to understand the different parts of the proposed functions of the connected intersection and how they interact; and

- Highlights a situation where an ambiguity or gap currently exists but will be addressed by the connected intersection.

5.6.1 Red Light Violation Warning (RLVW) Application

Title	Red Light Violation Warning (RLVW) Application – Green Extension Method
Background	Current connected vehicle RLVW applications focus exclusively on warning drivers of impending red light violations. In jurisdictions with a permissive yellow law (the majority of the U.S.), it is legal for vehicles to enter an intersection at any time during the yellow change interval and be in the intersection when the signal turns red. Consequently, some RLVW applications are designed to warn drivers who are likely to enter the intersection in red. It is activated on the vehicle by the OBUs and MUs at the beginning of the yellow change interval. This scenario describes CI/TSC infrastructure enhancements to the RLVW application for the through movements of an intersection by providing the following: a. Notification of the end of the green interval, providing more time for the in-vehicle RLVW application to perform its function, and b. The ability to add time to a green interval that helps the vehicle clear an intersection before the onset of red. Neither of these enhancements are possible in all cases. The CI/TSC infrastructure broadcasts a SPaT message containing the minimum and maximum end times for each signal group's current and next signal intervals to OBUs and MUs. These minimum and maximum end times may differ for green intervals, indicating uncertainty and variability about the end of green time. A higher degree of certainty regarding the end of green can be provided by an Assured Green End Time (AGET). An AGET is the time at which a timing green interval will terminate. It is conveyed through the SPaT message and represents the highest level of certainty about the end of green. Once set, an AGET can only be overridden due to preemption, equipment failure, or other factors outside the CI/TSC infrastructure's control. In fixed time signal control, where interval times are constant from cycle to cycle, an AGET can be set when the green interval begins. Providing an AGET is more difficult for actuated signal control where green interval times vary from cycle to cycle based on demand. For example, a through movement can be resting in green and terminate without setting an AGET due to demand on a cross street. In this case, the RLVW application on the vehicle must use the beginning of the yellow change interval to perform its function. An AGET may also be set seconds ahead of the actual end of the green interval, providing more opportunities for the in-vehicle RLVW application to warn a driver. This will depend on the type of signal control used by the intersection, the configuration, the demand for service, if an AGP is timing (see below), and other factors. The CI/TSC infrastructure can provide additional time to help vehicles approaching an intersection on through movements to clear an intersection before the onset of red. This is accomplished using an Assured Green Period (AGP). The AGP is an extension to a green interval that when combined with the yellow change interval is the time that a connected vehicle has to clear the intersection before the onset of red. The duration of the AGP is determined in advance using an assumed vehicle speed equal to the approach speed used to design the signal timing. To properly apply the AGP, the CI/TSC infrastructure needs to detect approaching connected vehicles (CVs). This is accomplished by IOOs defining and configuring a virtual advance detection zone called the RLVW Detection Zone (RDZ). There is an RDZ located upstream of the approach's designed stopping distance for each through movement of the intersection. The CI/TSC infrastructure receives Basic Safety Messages (BSMs) from all CVs within communications range of the connected intersection. The CI/TSC infrastructure uses the BSM data (e.g., location, speed, heading) to determine when a CV is located in the RDZ and moving toward the intersection. The CI/TSC infrastructure will use the AGP to extend the green interval of the through movement if all of the following are true: • An AGET has not been set. • The current time plus the AGP is greater than the minimum end time. • The current time plus the AGP is less than or equal to the maximum end time. The CI/TSC infrastructure may terminate a green interval for a through movement as part of the processing loop of its signal program, provided no AGP for the movement is being timed. CVs in or downstream of the RDZ will have received an AGP to help them clear the intersection before the beginning of red.

Title	Red Light Violation Warning (RLVW) Application – Green Extension Method
Summary of Operations	1) When a RLVW-equipped connected vehicle (CV) approaches a connected intersection, the OBU/MU receives signal timing (SPaT) and roadway geometry data (MAP) messages from the connected intersection and broadcasts the vehicle's location, speed, heading, and other data (BSM) to the CI/TSC infrastructure. 2) The CI/TSC infrastructure can set an AGET for a green interval of a through movement whenever it can be determined by the signal program. Once set, an AGET can only be overridden due to preemption, equipment failure, or other factors outside the TSC infrastructure's control. A signal program may terminate a green interval without setting an AGET. When a signal program is able to set an AGET (based on the type of signal control, configuration, demand, AGP, etc.), it may indicate an end of green seconds before it occurs, and provide more opportunities for the in-vehicle RLVW application to warn a driver. 3) The CI/TSC infrastructure can provide additional time to help vehicles approaching an intersection on through movements to clear an intersection before the onset of red. This is accomplished using an AGP. The AGP combined with the yellow change interval is the time that a connected vehicle has to clear the intersection before the onset of red. The duration of the AGP may be determined in advance using an assumed vehicle speed equal to the approach speed used to design the signal timing. 4) Using BSM data from CVs located in an RDZ, the CI/TSC infrastructure will set the minimum end time to the current time plus the AGP if all of the following are true: • An AGET has not been set. • The current time plus the AGP is greater than the minimum end time. • The current time plus the AGP is less than or equal to the maximum end time. 5) The CI/TSC infrastructure may terminate a green interval for a through movement as part of the processing loop of its signal program, provided no AGP is currently being timed. CVs in or downstream of the RDZ will have enough time to clear the intersection before the beginning of red.

5.6.2 Signal Timing Scenarios

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

5.6.2.1 Rest in Green

Title	Rest in Green
Summary of Operations	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. The connected intersection would either provide the following: • 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.

5.6.2.2 Two or More Signals or Intersections with One Controller

Title	**Two or More Signals or Intersections with One Controller**
Summary of Operations	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 use cases in this scenario are the following: 1. Two closely spaced intersections a. Texas Diamond b. Diverging Diamond (see Figure 7) 2. Box intersection (two divided highways crossing or frontage road intersections at a three-level diamond interchange) (see Figure 8) 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 9) 5. Signalized crosswalk close to the intersection 6. Michigan Left-Turn where the U-turn is signalized 7. Signalized roundabout
Graphics	

Figure 7 - Diverging diamond

Title	Two or More Signals or Intersections with One Controller

Figure 8 - Box intersection

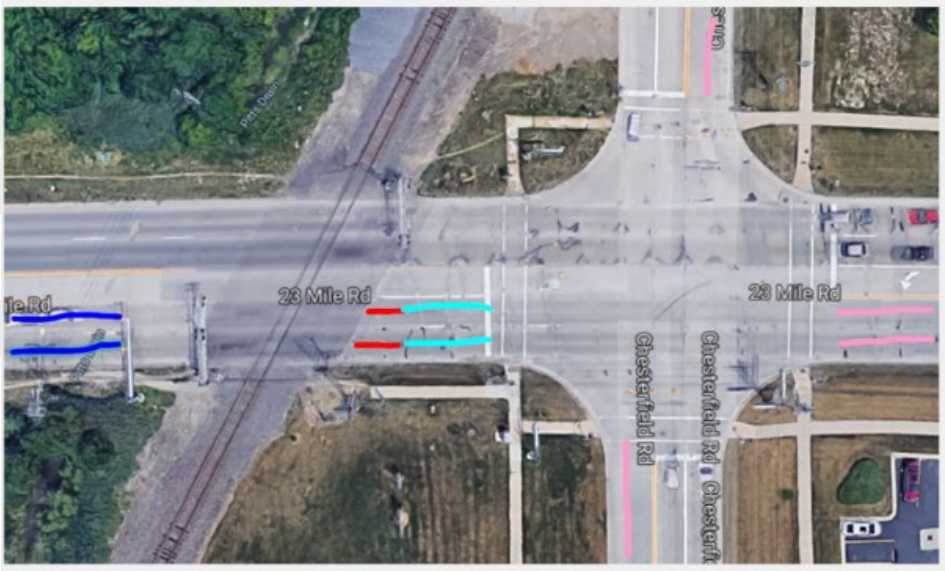
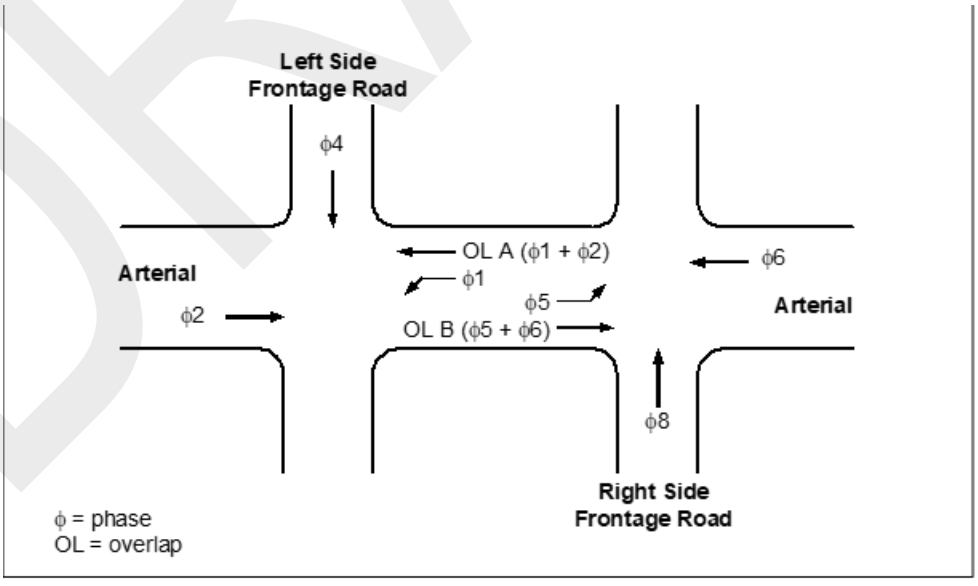


Figure 9 - Railroad crossing upstream of a signalized intersection

Source: Christopher Poe, Mixon Hill.

5.6.2.3 Texas Diamond Intersections

Title	Texas Diamond Intersections
Summary of Operations	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. Figure 10 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: • 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 is ON. • Overlap B (OL B) is an internal overlap that is ON when Phase 5 OR Phase 6 is ON. 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. • 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).
Graphics	 ***Figure 10 - Simplified phasing configuration for a texas diamond interchange***

Title	Texas Diamond Intersections
Needs	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 that is necessary to compile a SPaT message can be generated by the traffic signal controller. MAP Message Needs Texas Diamonds can vary in width. Due to constraints of V2X 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.

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

5.6.2.4 Florida T Intersection

Title	Florida T Intersection
Summary of Operations	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. Florida T intersections can also be signalized when needed to create adequate gaps in traffic for turn movements into and out of the T-leg of the intersection. Even with signalization, one direction of through traffic can continue through the intersection without stopping. Two examples are shown below; one without pedestrian crossings (see Figure 11), one with pedestrian crossings (see Figure 12). Each presents questions on whether or not the current timing parameters account for these uncertainties/complications: Summary of considerations for this scenario include the following: • How does a phase resting indefinitely report min time, max time, 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: o The controller (if in coordination) will now transition, making confidence go down. o 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.

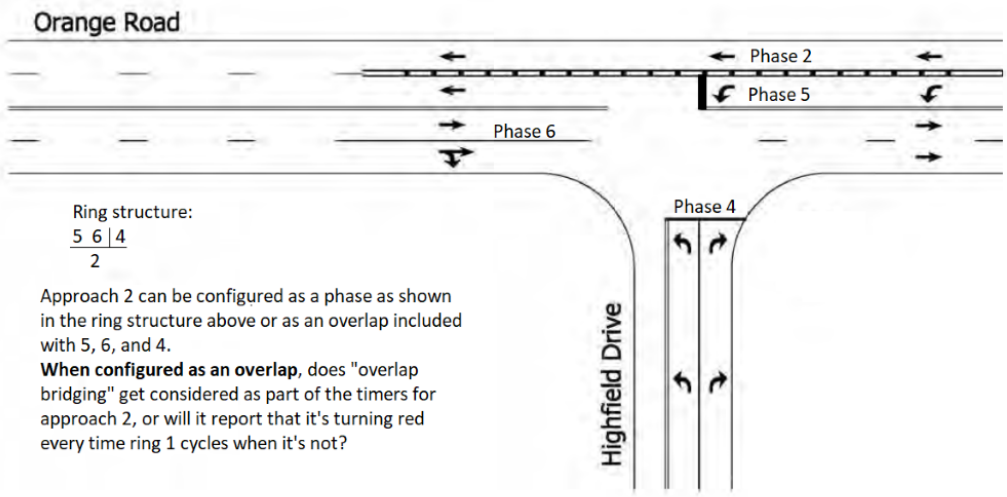
Title	Florida T Intersection
Graphics	

Figure 11 - Florida-T without pedestrian crossings

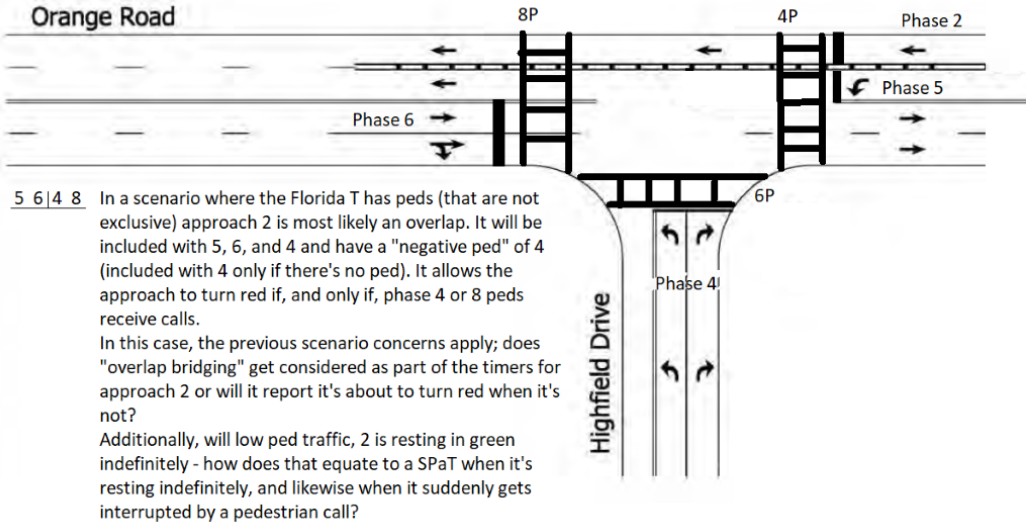


Figure 12 - Florida-T with pedestrian crossings

Source: Whitney Nottage, Intelight.

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

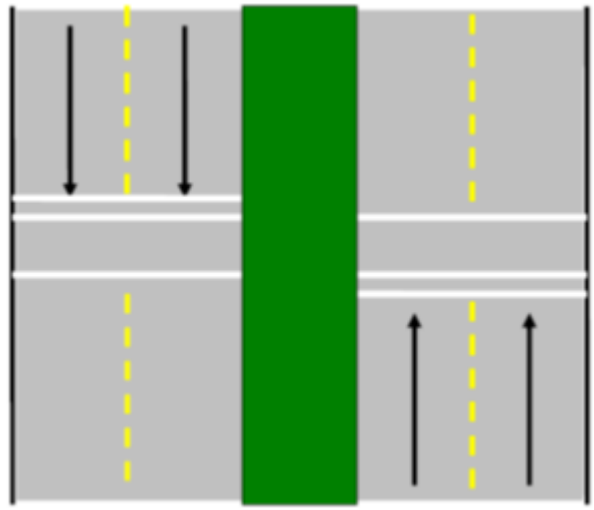
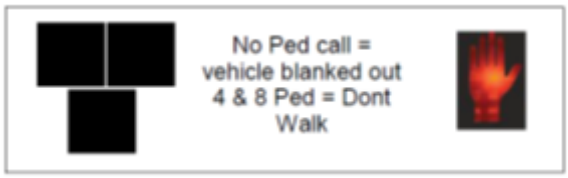
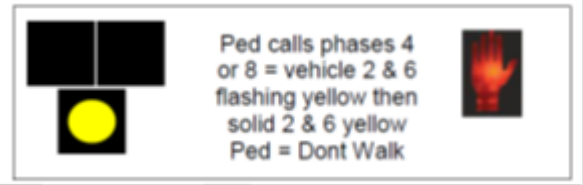
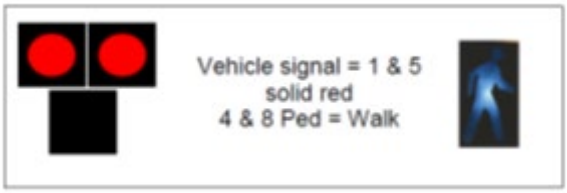
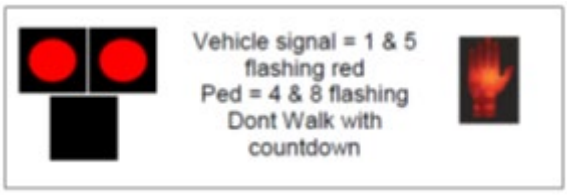
Title	**User Logic - Outside the "Knowledge" of the controller** Note: MultiModal Intelligent Traffic Signal System (MMITSS) and V2X Hub are common examples of external operations.
Summary of Operations	Definition: Outside the knowledge of the controller. This implies external manipulation of the actual 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. Examples of such external control "operations" might include the following: • NEMA Control Commands ○ 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 receipt of the command – i.e., it terminates a phase (FORCE-OFF) or skips a phase (OMIT). The excerpt below is from NTCIP 1202: "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." Examples of the commands supported are listed in NTCIP 1202: *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 }* *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 traffic 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.)

Title	User Logic - Outside the "Knowledge" of the controller
	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 1: It may be necessary to require some changes to the traffic 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 2: 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.

5.6.2.6 High-Intensity Activated Crosswalk Beacon (HAWK)

Title	High-Intensity Activated Crosswalk Beacon (HAWK)
Summary of Operations	A HAWK signal uses traditional traffic signal and pedestrian signal indications at crosswalks not located at the intersection of two roadways to assist pedestrians 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: • 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.

Title	High-Intensity Activated Crosswalk Beacon (HAWK)
Graphics	 Initial State  Activation and Vehicle Clearance  Pedestrian Interval  Pedestrian Clearance 

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

5.6.2.7 Dynamic Lane Use

Title	Dynamic Lane Use
Summary of Operations	Issue: Infrastructure owner's 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. 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 driver's the allowable movement. Signal heads may go dark for off peak direction where use is prohibited. 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.
Graphics	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 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

Source: Matt D'Angelo, Gresham Smith.

5.7 Relationship to the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) [Informative]

This section describes which portions of the Architecture Reference for Cooperative and Intelligent Transportation, known as ARC-IT, are addressed by CTI 4501. 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 13 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 CTI 4501. See Figure 4 to identify which of these interfaces are addressed by CTI 4501. A Physical Object is a system or device that provides ITS functionality as part of ITS.

NOTE: ARC-IT uses the term "RSE" which includes the RSU and other hardware that are used to broadcast and receive messages, as opposed to just an RSU.

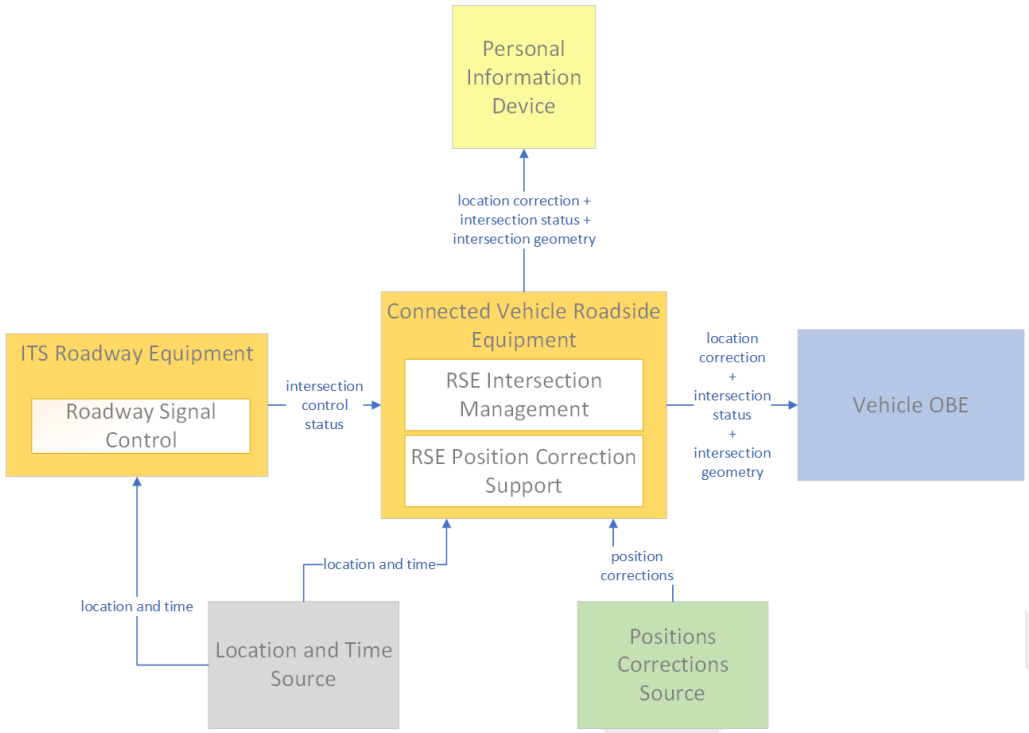


Figure 13 - ARC-IT physical view

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.

6. FUNCTIONAL REQUIREMENTS

Section 6 defines the Functional Requirements based on the user needs identified in the Concept of Operations (see Section 5). Section 6 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. The NRTM can also be used to define which requirements are to be tested (by demonstrating which requirements to be implemented).

c. Requirements: These are requirements that collectively satisfy the user needs identified in 5.4. These requirements provide the details so that a requirement can be fulfilled and validated.

Section 6 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 6 is useful in understanding the details of CTI 4501. For these readers, 6.2.3 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 CTI 4501. Table 5 in 6.2.3 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.

6.1 Tutorial [Informative]

This Functional Requirements section defines the formal requirements that are intended to satisfy the user needs identified in 5.4. This is achieved through the development of an 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.

6.2 Needs to Requirements Traceability Matrix (NRTM)

The NRTM, provided in 6.2.3, maps the user needs defined in Section 5 to the requirements defined in Section 6. The NRTM can be used by the following:

a. A user or specification writer to indicate which requirements are to be implemented (i.e., supported) 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

6.2.1 Notation

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.

6.2.1.1 Conformance Symbols

The symbols in Table 1 are used to indicate status under the Conformance column in the NRTM.

Table 1 - 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
MO	Mandatory to be implemented, optional to be used

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." So for example, in the NRTM below, requirement CTI 4501/1: 6.3.3.3.1.3, Road Authority Identifier, is MO in the Conformance column. This indicates that a conformant implementation must support Road Authority Identifier, but it is not required to be transmitted in the relevant messages.

6.2.1.2 Conditional Status Notation

The predicate notations in in Table 2 may be used.

Table 2 - 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 document map to the sections indicated in Table 3.

Table 3 - Predicate mapping

Predicate	Section
BSM	5.4.2.3.3
MAP	6.3.3.1.1.5
Misbehave	6.3.4.4.4
RLVW	5.4.2.3
RTCM	5.4.3.5
SPaT	6.3.3.1.1.1

6.2.1.3 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 4 - Support column entries

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

6.2.2 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.

6.2.2.1 Conformance Definition

To claim "Conformance" to this implementation guide, the manufacturer shall minimally fulfill the mandatory requirements as identified in the NRTM (see Table 5).

The reader and user of this implementation guide is advised that "conformance" to CTI 4501 should not be confused with "compliance" to a specification. CTI 4501 is as broad as possible to allow a very simple CI implementation to be "conformant." 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 specified in CTI 4501 to achieve interoperability. This means that functions and requirements specified as "optional" in CTI 4501 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 CTI 4501 and the standards it references (e.g., SAE J2735). For example, to claim conformance to additional features, an implementation shall conform to all 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).

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.

6.2.3 NRTM Table

Table 5 - Needs to requirements traceability matrix

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4	Needs					
5.4.1	Architectural Needs			M	Yes	
		6.3.1.1	LTE-V2X Traffic Class Settings	M	Yes	
		CTI 4501/1: 6.3.1.1.1.1	ProSe Per Packet Priority - SPaT Message	M	Yes	
		CTI 4501/2: 6.3.1.1.1.2	ProSe Per Packet Priority - MAP Message	M	Yes	
		SAE J3258: 6.1	LTE-V2X Settings	M	Yes	
		CTI 4501/1: 6.3.1.1.2.1	Transmit Radio - SPaT Message	M	Yes	
		CTI 4501/2: 6.3.1.1.2.2	Transmit Radio - MAP Message	M	Yes	
		CTI 4501/3: 6.3.4.1.51	Protect V2X Radio Parameters	M	Yes	
5.4.2	Traffic Signal Controller Infrastructure Data			M	Yes	
5.4.2.1	Provide Signal Timing Data to an RSU			M	Yes	
		CTI 4501/1: 6.3.2.1.1.1	NTCIP 1202 SPaT Information	O.1 (1)	Yes/No	
		CTI 4501/1: 6.3.2.1.1.2	TSCBM SPaT Information	O.1 (1)	Yes/No	Not recommended for new implementations
		CTI 4501/1: 6.3.2.1.1.3	SPaT Message - Immediate Forward	O.1 (1)	Yes/No	
		CTI 4501/1: 6.3.2.1.2	TSC Signal State Periodicity	M	Yes	
		CTI 4501/1: 6.3.2.1.3	TSC Signal Indication Phase State and SPaT Information Consistency	M	Yes	
5.4.2.2	Provide Signal Timing Status to an RSU			M	Yes	
		CTI 4501/1: 6.3.2.2.1	TSC Infrastructure Manual Control Indication	M	Yes	
		CTI 4501/1: 6.3.2.2.2	TSC Infrastructure Stop Time Indication	M	Yes	
		CTI 4501/1: 6.3.2.2.3	TSC Infrastructure Failure Flash (Exception Flash) Indication	M	Yes	
		CTI 4501/1: 6.3.2.2.4	TSC Infrastructure Preemption Operation Indication	M	Yes	
		CTI 4501/1: 6.3.2.2.5	TSC Infrastructure Priority Operation Indication	M	Yes	
		CTI 4501/1: 6.3.2.2.6	TSC Infrastructure Fixed Time Control Indication	M	Yes	
		CTI 4501/1: 6.3.2.2.7	TSC Infrastructure Traffic Dependent Control	M	Yes	
		CTI 4501/1: 6.3.2.2.8	TSC Infrastructure in Standby Mode	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.2.3 (RLVW)	RLVW Support			O	Yes/No	
5.4.2.3.1	Advance Notification of End of Green			M	Yes	
		CTI 4501/1: 6.3.2.3.1.1	AGET Known	M	Yes	
		CTI 4501/1: 6.3.2.3.1.2	AGET Undefined	M	Yes	
		CTI 4501/1: 6.3.2.3.2.1	AGP Extension	M	Yes	
		CTI 4501/1: 6.3.2.3.2.2	AGP Application	M	Yes	
		CTI 4501/1: 6.3.2.3.2.3	AGP Limited to Traffic Dependent Control	M	Yes	
5.4.2.3.2	Clear Intersection Before Onset of Red Indication			M	Yes	
		CTI 4501/1: 6.3.2.3.1.1	AGET Known	M	Yes	
		CTI 4501/1: 6.3.2.3.2.1	AGP Extension	M	Yes	
		CTI 4501/1: 6.3.2.3.2.2	AGP Application	M	Yes	
5.4.2.3.3 (BSM)	Receive Approaching Vehicle Information from an RSU			M	Yes	
		CTI 4501/1: 6.3.2.4.1	Receive BSM Messages	M	Yes	
		CTI 4501/1: 6.3.2.4.2	BSM Messages Filtered by Detection Zones	M	Yes	
		CTI 4501/1: 6.3.2.4.3	BSM Message Rate for AGP and RLVW	M	Yes	
		CTI 4501/3: 6.3.4.4.6	Security for Use of RSU BSM Filtering for RDZ	M	Yes	
		CTI 4501/3: 6.3.4.4.7	Security for Configuration of RSU BSM Filtering for RDZ	M	Yes	
5.4.3	Messages					
5.4.3.1	Message Performance Needs			M	Yes	
5.4.3.1.1	Uniform			M	Yes	
		CTI 4501/1: 6.3.3.1.1.1 (SPaT)	SPaT Message - SAE J2735	M	Yes	
		CTI 4501/1: 6.3.3.1.1.2	SPaT Message - Mandatory Data Elements	M	Yes	
		CTI 4501/1: 6.3.3.1.1.3	SPaT Message - Required Data Elements	M	Yes	
		CTI 4501/1: 6.3.3.1.1.4	SPaT Message PSID	M	Yes	
		CTI 4501/2: 6.3.3.1.1.5	MAP Message - SAE J2735	M	Yes	
		CTI 4501/2: 6.3.3.1.1.6	MAP Message - Mandatory Data Elements	M	Yes	
		CTI 4501/2: 6.3.3.1.1.7	MAP Message - Required Data Elements	M	Yes	
		CTI 4501/2: 6.3.3.1.1.8	MAP Message PSID	M	Yes	
		SAE J3258: 6.2.1	RTCMcorrections Message - SAE J2735	RTCM:M	Yes/NA	
		SAE J3258: 6.2.2	RTCMcorrections Message - Mandatory Data Elements	RTCM:M	Yes/NA	
		SAE J3258: 6.2.3	RTCMcorrections Message - Required Data Elements	RTCM:M	Yes/NA	
		SAE J3258: 6.2.4	RTCMcorrections Message PSID	RTCM:M	Yes/NA	
		CTI 4501/1: 6.3.3.1.1.13	BSM Message - SAE J2735	RLVW:M	Yes/NA	
		CTI 4501/1: 6.3.3.1.1.14	BSM Message PSID	RLVW:M	Yes/NA	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.3.1.2	Robustness			M	Yes	
		CTI 4501/1: 6.3.3.1.2.1	Broadcast SPaT Message	M	Yes	
		CTI 4501/1: 6.3.3.1.2.2	Continuous Broadcast of SPaT Messages	M	Yes	
		CTI 4501/1: 6.3.3.3.3.2	Unknown Current Movement State for a Signal Group	M	Yes	
		CTI 4501/1: 6.3.3.3.4.2	Unknown Next Movement State	M	Yes	
		CTI 4501/1: 6.3.3.3.5.2	Unknown Time Change Detail	M	Yes	
		CTI 4501/1: 6.3.3.3.5.5	Unknown Maximum End Time	M	Yes	
		CTI 4501/1: 6.3.3.3.5.6	Current Movement State Start Time Unknown	M	Yes	
5.4.3.1.3	Concise Messages			M	Yes	
		6.3.3.1.3.1	Transport Message Size - WAVE	M	Yes	
		CTI 4501/2: 6.3.3.1.3.2.1	Nodes by Offsets	M	Yes	
		CTI 4501/2: 6.3.3.1.3.2.2.1	Computed Lane - Lane Identifier	M	Yes	
		CTI 4501/2: 6.3.3.1.3.2.2.2	Computed Lane - X-Offset	M	Yes	
		CTI 4501/2: 6.3.3.1.3.2.2.3	Computed Lane - Y-Offset	M	Yes	
		CTI 4501/2: 6.3.3.1.3.2.2.4	Computed Lane - Angle	O	Yes/No	
5.4.3.1.4	Advanced Notification			M	Yes	
		6.3.3.1.4.1	Data Coverage - Every Ingress Lane	M	Yes	
		6.3.3.1.4.2	Advanced Notification - Time	M	Yes	
		CTI 4501/3: 6.3.4.17.1	Prevent Change in Radio Coverage	M	Yes	
		CTI 4501/3: 6.3.4.17.2	Detect Change in Radio Coverage	M	Yes	
		CTI 4501/3: 6.3.4.17.3	Prevent Change in Radio Power	M	Yes	
		CTI 4501/3: 6.3.4.17.4	Detect Change in Radio Power	M	Yes	
5.4.3.1.5	Timeliness			M	Yes	
		CTI 4501/1: 6.3.3.1.5.1	SPaT Message - Broadcast Latency and Accuracy	M	Yes	
		CTI 4501/1: 6.3.3.1.5.2	SPaT Message - Broadcast Periodicity	M	Yes	
		CTI 4501/2: 6.3.3.1.5.3	MAP Message - Broadcast Periodicity	M	Yes	
5.4.3.1.6	Quality Assurance			M	Yes	
		CTI 4501/1: 6.3.3.1.6.1	Completeness - SPaT Message	M	Yes	
		CTI 4501/2: 6.3.3.1.6.2	Completeness - MAP Message	M	Yes	
		CTI 4501/1: 6.3.3.1.6.3	SPaT Message - Time Mark Accuracy	M	Yes	
		CTI 4501/1: 6.3.3.3.2.13	No MAP Available	M	Yes	
		CTI 4501/1: 6.3.3.3.2.14	No SPaT Available	M	Yes	
		CTI 4501/1: 6.3.3.3.8	SPaT Message - Accuracy	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.3.2	Generic Message Data Needs					
5.4.3.2.1	Time Source			M	Yes	
		6.3.3.2.1	Time Accuracy	SPaT:M	Yes	
5.4.3.2.2	Message Revision			M	Yes	
		CTI 4501/1: 6.3.3.2.2.1	SPaT Message - Revision Counter Increment	M	Yes	
		CTI 4501/1: 6.3.3.2.2.2	SPaT Message - Revision Counter Not Increment	M	Yes	
		CTI 4501/2: 6.3.3.2.2.3	MAP Message - Revision Counter Increment	M	Yes	
		CTI 4501/2: 6.3.3.2.2.4	MAP Message - Revision Counter Not Increment	M	Yes	
		CTI 4501/2: 6.3.3.2.2.5	MAP Message - Intersection Revision Counter Increment	M	Yes	
		CTI 4501/2: 6.3.3.2.2.6	MAP Message - Intersection Revision Counter Not Increment	M	Yes	
		SAE J3258: 6.3.1	RTCMcorrections Message - Sequence Number Increment	RTCM:M	Yes/NA	
		SAE J3258: 6.3.2	RTCMcorrections Message - Sequence Number Not Increment	RTCM:M	Yes/NA	
5.4.3.2.3	Timestamp			M	Yes	
		CTI 4501/1: 6.3.3.2.3.1	SPaT Message - Message Timestamp	M	Yes	
		CTI 4501/1: 6.3.3.2.3.2	SPaT Message - Intersection Timestamp	M	Yes	
5.4.3.3	Signal Timing Data Needs			M	Yes	
5.4.3.3.1	Intersection Identification			M	Yes	
		CTI 4501/1: 6.3.3.3.1.1	Intersection Signal Timing Information	M	Yes	
		CTI 4501/1: 6.3.3.3.1.2	Intersection Identifier	M	Yes	
		CTI 4501/1: 6.3.3.3.1.3	Road Authority Identifier	MO	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.3.3.2	Intersection Status			M	Yes	
		CTI 4501/1: 6.3.3.1.2.1	Broadcast SPaT Message	M	Yes	
		CTI 4501/1: 6.3.3.3.2.1	Manual Control	M	Yes	
		CTI 4501/1: 6.3.3.3.2.2	Stop Time	M	Yes	
		CTI 4501/1: 6.3.3.3.2.3	Failure Flash	M	Yes	
		CTI 4501/1: 6.3.3.3.2.4	Preemption	M	Yes	
		CTI 4501/1: 6.3.3.3.2.5	Priority	M	Yes	
		CTI 4501/1: 6.3.3.3.2.6	Fixed Time	M	Yes	
		CTI 4501/1: 6.3.3.3.2.7	Traffic Dependent Mode	M	Yes	
		CTI 4501/1: 6.3.3.3.2.8	Standby Mode	M	Yes	
		CTI 4501/1: 6.3.3.3.2.9	Failure Mode	M	Yes	
		CTI 4501/1: 6.3.3.3.2.10	Controller Off	M	Yes	
		CTI 4501/1: 6.3.3.3.2.11	Recent MAP Update	M	Yes	
		CTI 4501/1: 6.3.3.3.2.12	New Lane IDs	M	Yes	
		CTI 4501/1: 6.3.3.3.2.13	No MAP Available	M	Yes	
		CTI 4501/1: 6.3.3.3.2.14	No SPaT Available	M	Yes	
		CTI 4501/1: 6.3.3.3.2.15	RTCM Corrections Available [Informative]	X	No	Proposed. Not Applicable at this time.
		CTI 4501/1: 6.3.3.3.2.16	Supports RLVW [Informative]	X	No	Proposed. Not Applicable at this time.
		CTI 4501/3: 6.3.4.11.1	Correctness of SPaT Availability Indications	M	Yes	
		CTI 4501/3: 6.3.4.11.2	Correctness of SPaT Unavailability Indications	M	Yes	
		CTI 4501/3: 6.3.4.11.3	Correctness of MAP Availability Indications	M	Yes	
		CTI 4501/3: 6.3.4.11.4	Correctness of MAP Unavailability Indications	M	Yes	
		CTI 4501/3: 6.3.4.11.5	Correctness of RTCM Availability Indications	M	Yes	
		CTI 4501/3: 6.3.4.11.6	Correctness of RTCM Unavailability Indications	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.3.3.3	Current Movement State			M	Yes	
		CTI 4501/1: 6.3.3.3.3.1	Current Movement State for a Signal Group	M	Yes	
		CTI 4501/1: 6.3.3.3.3.2	Unknown Current Movement State for a Signal Group	M	Yes	
		CTI 4501/1: 6.3.3.3.3.3	Flashing Yellow Arrow Permissive Movement	M	Yes	
		CTI 4501/1: 6.3.3.3.3.4	Protected and Permissive Clearance	M	Yes	
		CTI 4501/1: 6.3.3.3.3.5	Resolve Protected Versus Permissive Movement	M	Yes	
		CTI 4501/1: 6.3.3.3.3.6	Yield Causes Permissive	M	Yes	
		CTI 4501/1: 6.3.3.3.3.7	Right-of-Way Causes Protected	M	Yes	
		CTI 4501/1: 6.3.3.3.3.8	WALK State Enumeration	M	Yes	
		CTI 4501/1: 6.3.3.3.3.9	Flashing DON'T WALK State Enumeration	M	Yes	
		CTI 4501/1: 6.3.3.3.3.10	Steady DON'T WALK State Enumeration	M	Yes	
		CTI 4501/1: 6.3.3.3.3.11	Movement State for Signal Groups Identified	M	Yes	
		CTI 4501/1: 6.3.3.3.3.12	Dark Pedestrian Indications	M	Yes	
		CTI 4501/1: 6.3.3.3.3.13	Prohibited Movements	M	Yes	
		CTI 4501/1: 6.3.3.3.3.14	Movements Allowed After a Stop	M	Yes	
5.4.3.3.4	Next Movement State			M	Yes	
		CTI 4501/1: 6.3.3.3.4.1	Next Movement State	M	Yes	
		CTI 4501/1: 6.3.3.3.4.2	Unknown Next Movement State	M	Yes	
		CTI 4501/1: 6.3.3.3.4.3	No Past State	M	Yes	
5.4.3.3.5	Time Change Details			M	Yes	
		CTI 4501/1: 6.3.3.3.5.1	Time Change Details	M	Yes	
		CTI 4501/1: 6.3.3.3.5.2	Unknown Time Change Detail	M	Yes	
		CTI 4501/1: 6.3.3.3.5.3	Minimum End Time	M	Yes	
		CTI 4501/1: 6.3.3.3.5.4	Maximum End Time	M	Yes	
		CTI 4501/1: 6.3.3.3.5.5	Unknown Maximum End Time	M	Yes	
		CTI 4501/1: 6.3.3.3.5.6	Current Movement State Start Time Unknown	M	Yes	
		CTI 4501/1: 6.3.3.3.5.7	Next Movement State Start Time	M	Yes	
		CTI 4501/1: 6.3.3.3.5.8	Next State Start Time Equals Current State Minimum End Time	M	Yes	
5.4.3.3.6	Next Allowed Movement Time			M	Yes	
		CTI 4501/1: 6.3.3.3.6.1	Time of Next Allowed Movement	M	Yes	
5.4.3.3.7	Enabled Lanes			M	Yes	
		CTI 4501/1: 6.3.3.3.7	Enabled Lanes Indication	M	Yes	
5.4.3.3.8	Signal Timing and Roadway Indications Synchronization			M	Yes	
		CTI 4501/1: 6.3.3.1.5.1	SPaT Message - Broadcast Latency and Accuracy	M	Yes	
		CTI 4501/1: 6.3.3.3.8	SPaT Message - Accuracy	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.3.4	Roadway Geometry Data Needs			M	Yes	
5.4.3.4.1	Intersection Geometry			M	Yes	
		CTI 4501/2: 6.3.3.4.1.1	Intersection Geometry Information	M	Yes	
		CTI 4501/2: 6.3.3.4.1.2	Intersection Geometry - Road Authority Identifier	MO	Yes	
		CTI 4501/2: 6.3.3.4.1.3	Intersection Geometry - Intersection Identifier	M	Yes	
		CTI 4501/2: 6.3.3.4.1.4.1	Intersection Reference Point - Position	M	Yes	
		CTI 4501/2: 6.3.3.4.1.4.2	Intersection Reference Point - Description	M	Yes	
		CTI 4501/2: 6.3.3.4.1.5	Default Lane Width	M	Yes	
		CTI 4501/2: 6.3.3.4.1.6	Lane Identifier	M	Yes	
		CTI 4501/2: 6.3.3.4.1.7	Center of Vehicle Lane Geometry	M	Yes	
		CTI 4501/2: 6.3.3.4.1.8	Center of Crosswalk Lane Geometry	M	Yes	
		CTI 4501/2: 6.3.3.4.1.9	Center of Pedestrian Landings Geometry	M	Yes	
		CTI 4501/2: 6.3.3.4.1.10	Lane Description	M	Yes	
		CTI 4501/2: 6.3.3.4.1.11	First Node Point - Ingress Vehicle Lane	M	Yes	
		CTI 4501/2: 6.3.3.4.1.12	First Node Point - Egress Vehicle Lane	M	Yes	
		CTI 4501/2: 6.3.3.4.1.13	Node Offset from Intersection Reference Point	M	Yes	
		CTI 4501/2: 6.3.3.4.1.14	Node Elevation Offset from Intersection Reference Point	M	Yes	
		CTI 4501/2: 6.3.3.4.1.15	Offset from Previous Node	M	Yes	
		CTI 4501/2: 6.3.3.4.1.16	Elevation Offset from Previous Node	M	Yes	
		CTI 4501/2: 6.3.3.4.1.17	Advanced Notification - Ingress Vehicle Lane	M	Yes	
		CTI 4501/2: 6.3.3.4.1.18	End Nodes - Crosswalk Lane	M	Yes	
		CTI 4501/2: 6.3.3.4.1.19	End Nodes - Pedestrian Landing	M	Yes	
		CTI 4501/2: 6.3.3.4.1.20	Maximum Distance between Nodes	M	Yes	
		CTI 4501/2: 6.3.3.4.1.21	Maximum Number of Nodes	M	Yes	
		CTI 4501/2: 6.3.3.4.1.22	Node Lane Width	M	Yes	
		CTI 4501/2: 6.3.3.4.1.23	Node Lane Width Change	M	Yes	
5.4.3.4.2	Lane Attributes			M	Yes	
		CTI 4501/2: 6.3.3.4.2.1	Direction of Travel	M	Yes	
		CTI 4501/2: 6.3.3.4.2.2	Lane Sharing	MO	Yes	
		CTI 4501/2: 6.3.3.4.2.3	Lane Type Attributes	M	Yes	
		CTI 4501/2: 6.3.3.4.2.4	Lane Attributes - Vehicle	M	Yes	
		CTI 4501/2: 6.3.3.4.2.5	Lane Attributes - Crosswalk	MO	Yes	
		CTI 4501/2: 6.3.3.4.2.6	Lane Attributes - Bicycle	MO	Yes	
		CTI 4501/2: 6.3.3.4.2.7	Lane Attributes - Tracked Vehicles	MO	Yes	
		CTI 4501/2: 6.3.3.4.2.8	Lane Attributes - Parking	MO	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.3.4.3	Allowed Maneuvers			M	Yes	
		CTI 4501/2 6.3.3.4.3	Lane Maneuvers	M	Yes	
5.4.3.4.4	Connections Between Lanes			M	Yes	
		CTI 4501/2: 6.3.3.4.4.1	Lane Connections	M	Yes	
		CTI 4501/2: 6.3.3.4.4.2	Connection Egress Lane	M	Yes	
		CTI 4501/2: 6.3.3.4.4.3	Connection Maneuvers	O	Yes/No	
		CTI 4501/2: 6.3.3.4.4.4	Connection Signal Group	O	Yes/No	
		CTI 4501/2: 6.3.3.4.4.5	Include Only Permitted Connections	M	Yes	
5.4.3.4.5	Approach Speed Limit Information			MO	Yes	
		CTI 4501/2: 6.3.3.4.5.1	Default Speed Limit	M	Yes	
		CTI 4501/2: 6.3.3.4.5.2	Change in Lane Speed Limit	C	Yes/No	Mandatory if the speed limit changes on the approach
5.4.3.4.6	Revocable Lanes			MO	Yes	
		CTI 4501/2: 6.3.3.4.6	Revocable Lanes	M	Yes	
5.4.3.4.7	Road Geometry Accuracy			M	Yes	
		CTI 4501/2: 6.3.3.4.1.5	Default Lane Width	M	Yes	
		CTI 4501/2: 6.3.3.4.1.7	Center of Vehicle Lane Geometry	M	Yes	
		CTI 4501/2: 6.3.3.4.1.11	First Node Point - Ingress Vehicle Lane	M	Yes	
		CTI 4501/2: 6.3.3.4.1.12	First Node Point - Egress Vehicle Lane	M	Yes	
		CTI 4501/2: 6.3.3.4.1.18	End Nodes - Crosswalk Lane	M	Yes	
		CTI 4501/2: 6.3.3.4.1.19	End Nodes - Pedestrian Landing	M	Yes	
		CTI 4501/2: 6.3.3.4.1.20	Maximum Distance between Nodes	M	Yes	
		CTI 4501/2: 6.3.3.4.1.22	Node Lane Width	M	Yes	
		CTI 4501/2: 6.3.3.4.1.23	Node Lane Width Change	M	Yes	
5.4.3.4.8	Signal Timing and Roadway Geometry Synchronization			M	Yes	
		CTI 4501/1: 6.3.3.4.7.1	Matching SPaT and MAP Version	M	Yes	
		CTI 4501/1: 6.3.3.4.7.2	Matching Intersection Reference Identifiers	M	Yes	
		CTI 4501/1: 6.3.3.4.7.3	Complete List of Signal Group Identifiers	M	Yes	
		CTI 4501/1: 6.3.3.4.7.4	Matching Signal Group Identifier Movements	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.3.5 (RTCM)	Positioning Data Needs			O, M:2030	Yes/No	Proposed to be mandatory in year 2030. This allows IOOs time to provide RTCMcorrections at selected intersections.
5.4.3.5.1	Positioning Corrections Data Format			M	Yes	
		SAE J3258: 6.4.1.1	RTCM Version 3	M	Yes	
		SAE J3258: 6.4.1.2	RTCM Message Types	M	Yes	
		SAE J3258: 6.4.1.3	Geodetic Datum	M	Yes	
		SAE J3258: 6.4.1.4	RTCM Transport Layer Frame	M	Yes	
		SAE J3258: 6.4.1.5	Concatenation	M	Yes	
		SAE J3258: 6.4.1.6	Construction of SAE J2735 RTCMcorrections message	M	Yes	
		SAE J3258: 6.4.2	Minimum RTCM Corrections Broadcast Rate	M	Yes	
		SAE J3258: 6.4.3	WAVE Short Message Protocol	M	Yes	
5.4.3.5.2	Real-Time Kinematic Corrections			O	Yes/No	
		SAE J3258: 6.5.1	RTK Source Proximity	M	Yes	
		SAE J3258: 6.5.2	RTK Source Failure Handling	M	Yes	
5.4.3.6	Vehicle Data Needs			BSM:O	Yes/No/ NA	
5.4.3.6.1	Vehicle Position and Kinematics			M	Yes	
		CTI 4501/1: 6.3.3.6.1	Vehicle Position	M	Yes	
		CTI 4501/1: 6.3.3.6.2	Vehicle Kinematics	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4	Security					
5.4.4.1	Data Trustworthiness					
5.4.4.1.1	Data Trustworthiness: Sources			M	Yes	
		CTI 4501/3: 6.3.4.1.1	Internal Data Sources and Processing	M	Yes	
		CTI 4501/3: 6.3.4.1.2	Manual Data	M	Yes	
		CTI 4501/3: 6.3.4.1.3	Internal Manual Data Sources	M	Yes	
		CTI 4501/3: 6.3.4.1.4	Permitted Data from Manual Data Sources	M	Yes	
		CTI 4501/3: 6.3.4.1.5	External CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.6	Authorized CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.7	Authenticated CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.8	Integrity of Operations for Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.9	Integrity of Operational Mode for Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.10	Integrity of Operational Mode Indications for Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.11	Physical Access to Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.12	Physical Access to Internal CI Data Entities During Outages or Degraded Operations	M	Yes	
		CTI 4501/3: 6.3.4.1.13	Logical Access to Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.14	Logical Access to Internal CI Data Entities During Outages or Degraded Operations	M	Yes	
		CTI 4501/3: 6.3.4.1.15	Mitigate Malicious Access to Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.16	Access Control on Internal CI Data Entities During Life Cycle	M	Yes	
		CTI 4501/3: 6.3.4.1.17	Integrity of Operations for External CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.18	Mitigate Malicious Access to External Data Sources and Processing	M	Yes	
		CTI 4501/3: 6.3.4.1.19	Access Privileges for Data Sources and Processing	M	Yes	
		CTI 4501/3: 6.3.4.1.20	Access Privileges for Manually Entered Data	M	Yes	
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26	Self-Monitoring for Internal CI Data Entities: Robustness	M	Yes	
		CTI 4501/3: 6.3.4.1.27	Self-Monitoring for Internal CI Data Entities: Error Management	M	Yes	
		CTI 4501/3: 6.3.4.1.28	Recovery from Failure for Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.29	Assurance of Recovery from Failure for Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.30	Source Assurance for Recovery from Failure for Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.31	Automated Recovery from Failure for Internal CI Data Entities is Not to Be an Attack Vector	M	Yes	
		CTI 4501/3: 6.3.4.1.32	Self-Monitoring for Internal CI Data Entities: Logging	M	Yes	
		CTI 4501/3: 6.3.4.1.33	Log Generation for External CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.34	Log Events for CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.35	Changes in Logged Information	M	Yes	
		CTI 4501/3: 6.3.4.1.36	Access to Logs for CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.37	Timely Access to Logs for CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.38	List of Communications Nodes on which Data Could Be Modified	M	Yes	
		CTI 4501/3: 6.3.4.1.39	Communications Nodes on which Data is Manipulable Count as Data Transformation Components	M	Yes	
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	
		CTI 4501/3: 6.3.4.1.52	Threat Analysis	M	Yes	
		CTI 4501/3: 6.3.4.3.x	Trustworthiness of TSC-originating Information	M	Yes	All child requirements are mandatory but not listed to conserve space.

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.4.1	Validate Security of Approaching Vehicle V2X Messages	BSM:M	Yes/NA	
		CTI 4501/3: 6.3.4.4.2	Validate Approaching Vehicle V2X Messages: Replay	BSM:M	Yes/NA	
		CTI 4501/3: 6.3.4.4.3	Validate Approaching Vehicle V2X Messages: Misbehavior Detection	BSM:O	Yes/No/ NA	
		CTI 4501/3: 6.3.4.4.4 (Misbehave)	Validate Approaching Vehicle V2X Messages: Misbehavior Reporting	BSM:O	Yes/No/ NA	
		CTI 4501/3: 6.3.4.4.5	Validate Approaching Vehicle V2X Messages: Distinguish Between Senders	Misbehave:M	Yes/No/ NA	
		CTI 4501/3: 6.3.4.5.1	Validation of Approaching Vehicle Information by TSC	BSM:M	Yes/NA	
		CTI 4501/3: 6.3.4.5.2	Protection from Unnecessary AGP	O	Yes	
		CTI 4501/3: 6.3.4.6.1	Availability of Time Sources	M	Yes	
		CTI 4501/3: 6.3.4.6.2	Detect Time Source Delay	M	Yes	
		CTI 4501/3: 6.3.4.6.3	Manage Time Source Delay	M	Yes	
		CTI 4501/3: 6.3.4.6.4	Time Source Delay for External Time Sources	M	Yes	
		CTI 4501/3: 6.3.4.6.5	Time Source Delay for External Time Sources: Other Users	M	Yes	
		CTI 4501/3: 6.3.4.7.1	List of CI Data Entities that affect SPaT Contents	M	Yes	
		CTI 4501/3: 6.3.4.7.2	Prevent invalid SPaT Contents or Behavior	M	Yes	
		CTI 4501/3: 6.3.4.7.3	Detect Inconsistency of SPaT and Signal Timing Data	M	Yes	
		CTI 4501/3: 6.3.4.7.4	Manage Inconsistency of SPaT and Signal Timing Data	M	Yes	
		CTI 4501/3: 6.3.4.8.1	List of CI Data Entities that Affect MAP Contents	M	Yes	
		CTI 4501/3: 6.3.4.8.2	Prevent Invalid MAP Contents or Behavior	O.5 (1..*)	Yes/No	Applies only if the MAP is generated inside the CI.
		CTI 4501/3: 6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source	O.5 (1..*)	Yes/No	Applies only if the MAP is generated outside the CI.
		CTI 4501/3: 6.3.4.8.4	Prevent Inconsistency of MAP and Road Geometry or Use: False Positives	M	Yes	
		CTI 4501/3: 6.3.4.8.5	Prevent Inconsistency of MAP and Road Geometry or Use: False Negatives	M	Yes	
		CTI 4501/3: 6.3.4.8.6	Detect Inconsistency of MAP and Road Geometry or Use	M	Yes	
		CTI 4501/3: 6.3.4.8.7	Manage Inconsistency of MAP and Road Geometry or Use	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.9.1	List of CI Data Entities that Affect RTCM Contents	RLVW:M	Yes/NA	
		CTI 4501/3: 6.3.4.9.2	Prevent Invalid RTCM Contents or Behavior	RLVW:O.6 (1..*)	Yes/No/ NA	Applies only if the RTCM is generated inside the CI.
		CTI 4501/3: 6.3.4.9.3	External RTCM Message Generation or Partial Generation: Data Source	RLVW:O.6 (1..*)	Yes/No/ NA	Applies only if any RTCM data is generated outside the CI.
5.4.4.1.2	Data Trustworthiness: Processing					
		CTI 4501/3: 6.3.4.1.1	Internal Data Sources and Processing	M	Yes	
		CTI 4501/3: 6.3.4.1.5	External CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.6	Authorized CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.7	Authenticated CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.8	Integrity of Operations for Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.9	Integrity of Operational Mode for Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.10	Integrity of Operational Mode Indications for Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.11	Physical Access to Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.12	Physical Access to Internal CI Data Entities During Outages or Degraded Operations	M	Yes	
		CTI 4501/3: 6.3.4.1.13	Logical Access to Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.14	Logical Access to Internal CI Data Entities During Outages or Degraded Operations	M	Yes	
		CTI 4501/3: 6.3.4.1.15	Mitigate Malicious Access to Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.16	Access Control on Internal CI Data Entities During Life Cycle	M	Yes	
		CTI 4501/3: 6.3.4.1.17	Integrity of Operations for External CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.18	Mitigate Malicious Access to External Data Sources and Processing	M	Yes	
		CTI 4501/3: 6.3.4.1.19	Access Privileges for Data Sources and Processing	M	Yes	
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	
		CTI 4501/3: 6.3.4.1.52	Threat Analysis	M	Yes	
		CTI 4501/3: 6.3.4.3.x	Trustworthiness of TSC-originating Information	M	Yes	All child requirements are mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.4.1	Validate Approaching Vehicle V2X Messages	BSM:M	Yes/NA	
		CTI 4501/3: 6.3.4.4.2	Validate Approaching Vehicle V2X Messages: Replay	BSM:M	Yes/NA	
		CTI 4501/3: 6.3.4.4.3	Validate Approaching Vehicle V2X Messages: Misbehavior Detection	BSM:O	Yes/No/ NA	
		CTI 4501/3: 6.3.4.4.4 (Misbehave)	Validate Approaching Vehicle V2X Messages: Misbehavior Reporting	BSM:O	Yes/No/ NA	
		CTI 4501/3: 6.3.4.4.5	Validate Approaching Vehicle V2X Messages: Distinguish Between Senders	Misbehave:M	Yes/No/ NA	
		CTI 4501/3: 6.3.4.5.1	Validation of Approaching Vehicle Information by TSC	BSM:M	Yes/NA	
		CTI 4501/3: 6.3.4.5.2	Protection from Unnecessary AGP	O	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.6.x	Time Source Trustworthiness	M	Yes	All child requirements are mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.7.x	SPaT Message Trustworthiness and Reliability	M	Yes	All child requirements are mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.8.1	List of CI Data Entities that Affect MAP Contents	M	Yes	
		CTI 4501/3: 6.3.4.8.2	Prevent Invalid MAP Contents or Behavior	O.5 (1..*)	Yes/No	Applies only if the MAP is generated inside the CI.
		CTI 4501/3: 6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source	O.5 (1..*)	Yes/No	Applies only if the MAP is generated outside the CI.
		CTI 4501/3: 6.3.4.8.4	Prevent Inconsistency of MAP and Road Geometry or Use: False Positives	M	Yes	
		CTI 4501/3: 6.3.4.8.5	Prevent Inconsistency of MAP and Road Geometry or Use: False Negatives	M	Yes	
		CTI 4501/3: 6.3.4.8.6	Detect Inconsistency of MAP and Road Geometry or Use	M	Yes	
		CTI 4501/3: 6.3.4.8.7	Manage Inconsistency of MAP and Road Geometry or Use	M	Yes	
		CTI 4501/3: 6.3.4.9.1	List of CI Data Entities that Affect RTCM Contents	RLVW:M	Yes/NA	
		CTI 4501/3: 6.3.4.9.2	Prevent Invalid RTCM Contents or Behavior	RLVW:M	Yes/NA	
		CTI 4501/3: 6.3.4.9.3	External RTCM Message Generation or Partial Generation: Data Source	RLVW:M	Yes/NA	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.1.3.1	Signal Timing Data Trustworthiness			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.3.x	Trustworthiness of TSC-originating Information	M	Yes	All child requirements are mandatory but not listed to conserve space.
5.4.4.1.3.2	Signal Timing Status Trustworthiness			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.3.x	Trustworthiness of TSC-originating Information	M	Yes	All child requirements are mandatory but not listed to conserve space.

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.1.3.3	Approaching Vehicle Information Trustworthiness: RSU			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.4.1	Validate Approaching Vehicle V2X Messages	BSM:M	Yes/NA	
		CTI 4501/3: 6.3.4.4.2	Validate Approaching Vehicle V2X Messages: Replay	BSM:M	Yes/NA	
		CTI 4501/3: 6.3.4.4.3	Validate Approaching Vehicle V2X Messages: Misbehavior Detection	BSM:O	Yes/No/ NA	
		CTI 4501/3: 6.3.4.4.4 (Misbehave)	Validate Approaching Vehicle V2X Messages: Misbehavior Reporting	BSM:O	Yes/No/ NA	
		CTI 4501/3: 6.3.4.4.5	Validate Approaching Vehicle V2X Messages: Distinguish Between Senders	Misbehave:M	Yes/No/ NA	
5.4.4.1.3.4	Approaching Vehicle Information Trustworthiness: TSC			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.5.1	Validation of Approaching Vehicle Information by TSC	BSM:M	Yes/NA	
		CTI 4501/3: 6.3.4.5.2	Protection from Unnecessary AGP	O	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.1.3.5	Time Source Trustworthiness					
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.6.x	Time Source Trustworthiness	M	Yes	All child requirements are mandatory but not listed to conserve space.
5.4.4.1.3.6	Message Revision Trustworthiness			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.7.1	List of CI Data Entities that affect SPaT Contents	M	Yes	
		CTI 4501/3: 6.3.4.7.2	Prevent invalid SPaT Contents or Behavior	M	Yes	
		CTI 4501/3: 6.3.4.8.1	List of CI Data Entities that Affect MAP Contents	M	Yes	
		CTI 4501/3: 6.3.4.8.2	Prevent Invalid MAP Contents or Behavior	M	Yes	
		CTI 4501/3: 6.3.4.9.1	List of CI Data Entities that Affect RTCM Contents	M	Yes	
		CTI 4501/3: 6.3.4.9.2	Prevent Invalid RTCM Contents or Behavior	RLVW:M	Yes/NA	
		CTI 4501/3: 6.3.4.10.1	SPaT and MAP Version Consistency	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.1.3.7	Timestamp Trustworthiness			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.6.x	Time Source Trustworthiness	M	Yes	All child requirements are mandatory but not listed to conserve space.
5.4.4.1.3.8	Intersection Identifier Trustworthiness			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.7.1	List of CI Data Entities that affect SPaT Contents	M	Yes	
		CTI 4501/3: 6.3.4.7.2	Prevent invalid SPaT Contents or Behavior	M	Yes	
		CTI 4501/3: 6.3.4.8.1	List of CI Data Entities that Affect MAP Contents	M	Yes	
		CTI 4501/3: 6.3.4.8.2	Prevent Invalid MAP Contents or Behavior	M	Yes	
		CTI 4501/3: 6.3.4.12.1	Robustness of Intersection Identifier Assignment	M	Yes	
		CTI 4501/3: 6.3.4.12.2	Detect Incorrect Intersection Identifiers	O	Yes/No	
		CTI 4501/3: 6.3.4.12.3	Manage Incorrect Intersection Identifiers	O	Yes/No	
		CTI 4501/3: 6.3.4.12.4	Detect Duplicate Use of Intersection Identifiers by External Parties	O	Yes/No	
		CTI 4501/3: 6.3.4.12.5	Manage Duplicate Use of Intersection Identifiers by External Parties	O	Yes/No	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.1.3.9	Intersection Status Trustworthiness			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.3.x	Trustworthiness of TSC-originating Information	M	Yes	All child requirements are mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.7.1	List of CI Data Entities that affect SPaT Contents	M	Yes	
		CTI 4501/3: 6.3.4.7.2	Prevent invalid SPaT Contents or Behavior	M	Yes	
5.4.4.1.3.10	Current Movement State Trustworthiness			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.3.x	Trustworthiness of TSC-originating Information	M	Yes	All child requirements are mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.7.1	List of CI Data Entities that affect SPaT Contents	M	Yes	
		CTI 4501/3: 6.3.4.7.2	Prevent invalid SPaT Contents or Behavior	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.1.3.11	Next Movement State Trustworthiness			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.3.x	Trustworthiness of TSC-originating Information	M	Yes	All child requirements are mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.7.1	List of CI Data Entities That Affect SPaT Contents	M	Yes	
		CTI 4501/3: 6.3.4.7.2	Prevent invalid SPaT Contents or Behavior	M	Yes	
5.4.4.1.3.12	Time Change Details Trustworthiness			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.3.x	Trustworthiness of TSC-originating Information	M	Yes	All child requirements are mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.7.1	List of CI Data Entities that affect SPaT Contents	M	Yes	
		CTI 4501/3: 6.3.4.7.2	Prevent invalid SPaT Contents or Behavior	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.1.3.13	Next Allowed Movement Time Trustworthiness			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.3.x	Trustworthiness of TSC-originating Information	M	Yes	All child requirements are mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.7.1	List of CI Data Entities that affect SPaT Contents	M	Yes	
		CTI 4501/3: 6.3.4.7.2	Prevent invalid SPaT Contents or Behavior	M	Yes	
5.4.4.1.3.14	Enabled Lanes Trustworthiness			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.3.x	Trustworthiness of TSC-originating Information	M	Yes	All child requirements are mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.7.1	List of CI Data Entities that affect SPaT Contents	M	Yes	
		CTI 4501/3: 6.3.4.7.2	Prevent invalid SPaT Contents or Behavior	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.1.3.15	Signal Timing and Roadway Indications Synchronization Trustworthiness: Robustness			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.3.x	Trustworthiness of TSC-originating Information	M	Yes	All child requirements are mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.7.x	SPaT Message Trustworthiness and Reliability	M	Yes	All child requirements are mandatory but not listed to conserve space.
5.4.4.1.3.16	Signal Timing and Roadway Indications Synchronization Trustworthiness: Correct Information			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.3.x	Trustworthiness of TSC-originating Information	M	Yes	All child requirements are mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.7.x	SPaT Message Trustworthiness and Reliability	M	Yes	All child requirements are mandatory but not listed to conserve space.

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.1.3.17	Intersection Geometry Trustworthiness			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.8.2	Prevent Invalid MAP Contents or Behavior	O.5 (1..*)	Yes/No	Applies only if the MAP is generated inside the CI.
		CTI 4501/3: 6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source	O.5 (1..*)	Yes/No	Applies only if the MAP is generated outside the CI.
		CTI 4501/3: 6.3.4.8.4	Prevent Inconsistency of MAP and Road Geometry or Use: False Positives	M	Yes	
		CTI 4501/3: 6.3.4.8.5	Prevent Inconsistency of MAP and Road Geometry or Use: False Negatives	M	Yes	
		CTI 4501/3: 6.3.4.8.6	Detect Inconsistency of MAP and Road Geometry or Use	M	Yes	
		CTI 4501/3: 6.3.4.8.7	Manage Inconsistency of MAP and Road Geometry or Use	M	Yes	
5.4.4.1.3.18	Lane Attributes Trustworthiness			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.8.1	List of CI Data Entities that Affect MAP Contents	M	Yes	
		CTI 4501/3: 6.3.4.8.2	Prevent Invalid MAP Contents or Behavior	O.5 (1..*)	Yes/No	Applies only if the MAP is generated inside the CI.

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source	O.5 (1..*)	Yes/No	Applies only if the MAP is generated outside the CI.
		CTI 4501/3: 6.3.4.8.4	Prevent Inconsistency of MAP and Road Geometry or Use: False Positives	M	Yes	
		CTI 4501/3: 6.3.4.8.5	Prevent Inconsistency of MAP and Road Geometry or Use: False Negatives	M	Yes	
		CTI 4501/3: 6.3.4.8.6	Detect Inconsistency of MAP and Road Geometry or Use	M	Yes	
		CTI 4501/3: 6.3.4.8.7	Manage Inconsistency of MAP and Road Geometry or Use	M	Yes	
5.4.4.1.3.19	Allowed Maneuvers Trustworthiness			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.8.1	List of CI Data Entities that Affect MAP Contents	M	Yes	
		CTI 4501/3: 6.3.4.8.2	Prevent Invalid MAP Contents or Behavior	O.5 (1..*)	Yes/No	Applies only if the MAP is generated inside the CI.
		CTI 4501/3: 6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source	O.5 (1..*)	Yes/No	Applies only if the MAP is generated outside the CI.
		CTI 4501/3: 6.3.4.8.4	Prevent Inconsistency of MAP and Road Geometry or Use: False Positives	M	Yes	
		CTI 4501/3: 6.3.4.8.5	Prevent Inconsistency of MAP and Road Geometry or Use: False Negatives	M	Yes	
		CTI 4501/3: 6.3.4.8.6	Detect Inconsistency of MAP and Road Geometry or Use	M	Yes	
		CTI 4501/3: 6.3.4.8.7	Manage Inconsistency of MAP and Road Geometry or Use	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.1.3.20	Connections Between Lanes Trustworthiness			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.8.1	List of CI Data Entities that Affect MAP Contents	M	Yes	
		CTI 4501/3: 6.3.4.8.2	Prevent Invalid MAP Contents or Behavior	O.5 (1..*)	Yes/No	Applies only if the MAP is generated inside the CI.
		CTI 4501/3: 6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source	O.5 (1..*)	Yes/No	Applies only if the MAP is generated outside the CI.
		CTI 4501/3: 6.3.4.8.4	Prevent Inconsistency of MAP and Road Geometry or Use: False Positives	M	Yes	
		CTI 4501/3: 6.3.4.8.5	Prevent Inconsistency of MAP and Road Geometry or Use: False Negatives	M	Yes	
		CTI 4501/3: 6.3.4.8.6	Detect Inconsistency of MAP and Road Geometry or Use	M	Yes	
		CTI 4501/3: 6.3.4.8.7	Manage Inconsistency of MAP and Road Geometry or Use	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.1.3.21	Approach Speed Limits Trustworthiness			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.8.1	List of CI Data Entities that Affect MAP Contents	M	Yes	
		CTI 4501/3: 6.3.4.8.2	Prevent Invalid MAP Contents or Behavior	O.5 (1..*)	Yes/No	Applies only if the MAP is generated inside the CI.
		CTI 4501/3: 6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source	O.5 (1..*)	Yes/No	Applies only if the MAP is generated outside the CI.
		CTI 4501/3: 6.3.4.8.4	Prevent Inconsistency of MAP and Road Geometry or Use: False Positives	M	Yes	
		CTI 4501/3: 6.3.4.8.5	Prevent Inconsistency of MAP and Road Geometry or Use: False Negatives	M	Yes	
		CTI 4501/3: 6.3.4.8.6	Detect Inconsistency of MAP and Road Geometry or Use	M	Yes	
		CTI 4501/3: 6.3.4.8.7	Manage Inconsistency of MAP and Road Geometry or Use	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.1.3.22	Revocable Lanes Trustworthiness			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.8.1	List of CI Data Entities that Affect MAP Contents	M	Yes	
		CTI 4501/3: 6.3.4.8.2	Prevent Invalid MAP Contents or Behavior	O.5 (1..*)	Yes/No	Applies only if the MAP is generated inside the CI.
		CTI 4501/3: 6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source	O.5 (1..*)	Yes/No	Applies only if the MAP is generated outside the CI.
		CTI 4501/3: 6.3.4.8.4	Prevent Inconsistency of MAP and Road Geometry or Use: False Positives	M	Yes	
		CTI 4501/3: 6.3.4.8.5	Prevent Inconsistency of MAP and Road Geometry or Use: False Negatives	M	Yes	
		CTI 4501/3: 6.3.4.8.6	Detect Inconsistency of MAP and Road Geometry or Use	M	Yes	
		CTI 4501/3: 6.3.4.8.7	Manage Inconsistency of MAP and Road Geometry or Use	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.1.3.23	Road Geometry Accuracy Trustworthiness			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.8.1	List of CI Data Entities that Affect MAP Contents	M	Yes	
		CTI 4501/3: 6.3.4.8.2	Prevent Invalid MAP Contents or Behavior	O.5 (1..*)	Yes/No	Applies only if the MAP is generated inside the CI.
		CTI 4501/3: 6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source	O.5 (1..*)	Yes/No	Applies only if the MAP is generated outside the CI.
		CTI 4501/3: 6.3.4.8.4	Prevent Inconsistency of MAP and Road Geometry or Use: False Positives	M	Yes	
		CTI 4501/3: 6.3.4.8.5	Prevent Inconsistency of MAP and Road Geometry or Use: False Negatives	M	Yes	
		CTI 4501/3: 6.3.4.8.6	Detect Inconsistency of MAP and Road Geometry or Use	M	Yes	
		CTI 4501/3: 6.3.4.8.7	Manage Inconsistency of MAP and Road Geometry or Use	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.1.3.24	Signal Timing and Roadway Geometry Synchronization Trustworthiness			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.8.1	List of CI Data Entities that Affect MAP Contents	M	Yes	
		CTI 4501/3: 6.3.4.8.2	Prevent Invalid MAP Contents or Behavior	O.5 (1..*)	Yes/No	Applies only if the MAP is generated inside the CI.
		CTI 4501/3: 6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source	O.5 (1..*)	Yes/No	Applies only if the MAP is generated outside the CI.
		CTI 4501/3: 6.3.4.8.4	Prevent Inconsistency of MAP and Road Geometry or Use: False Positives	M	Yes	
		CTI 4501/3: 6.3.4.8.5	Prevent Inconsistency of MAP and Road Geometry or Use: False Negatives	M	Yes	
		CTI 4501/3: 6.3.4.8.6	Detect Inconsistency of MAP and Road Geometry or Use	M	Yes	
		CTI 4501/3: 6.3.4.8.7	Manage Inconsistency of MAP and Road Geometry or Use	M	Yes	
		CTI 4501/3: 6.3.4.10.1	SPaT and MAP Version Consistency	M	Yes	
		CTI 4501/3: 6.3.4.10.2	SPaT and MAP Intersection Identifier Consistency	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.1.3.25	RTK Corrections Message Trustworthiness			RTCM:M	Yes/NA	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.9.1	List of CI Data Entities that Affect RTCM Contents	M	Yes	
		CTI 4501/3: 6.3.4.9.2	Prevent Invalid RTCM Contents or Behavior	M	Yes	
		CTI 4501/3: 6.3.4.9.3	External RTCM Message Generation or Partial Generation: Data Source	M	Yes	
5.4.4.2	Security Needs: Data In Transit					
5.4.4.2.1	Integrity Of Data Passing Across Interfaces Within the CI			M	Yes	
		CTI 4501/3: 6.3.4.2.3	Secure Communications: Integrity	M	Yes	
5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI			M	Yes	
		CTI 4501/3: 6.3.4.1.1 to CTI 4501/3: 6.3.4.1.20	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.1 – 6.3.4.1.20 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.21	Record of Accesses to CI Data Entities	O	Yes/No	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.1.26 to CTI 4501/3: 6.3.4.1.39	Data Trustworthiness: Sources and Processing Requirements	M	Yes	Requirements CTI 4501/3: 6.3.4.1.26 – 6.3.4.1.39 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	
		CTI 4501/3: 6.3.4.2.1 to CTI 4501/3: 6.3.4.2.23 except CTI 4501/3 6.3.4.2.8	Data Communications Security	M	Yes	Requirements CTI 4501/3: 6.3.4.2.1 – 6.3.4.2.23 except 6.3.4.2.8 are all mandatory but not listed to conserve space.
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.2.24	Protection of Cryptographic Keying Material: General	M	Yes	
		CTI 4501/3: 6.3.4.2.25	Protection of Cryptographic Keying Material: Hardware	M	Yes	
		CTI 4501/3: 6.3.4.2.26	Protection of Cryptographic Keying Material: Access to and Use of Keys	M	Yes	
5.4.4.2.3	Integrity Of Messages Sent From CI			M	Yes	
		CTI 4501/3: 6.3.4.2.4	Secure Communications: Integrity of External CI Data Outbound Logical Interfaces	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.3	Security Needs: Resilience					
5.4.4.3.1	Data Sources: Resilience			M	Yes	
		CTI 4501/3: 6.3.4.1.15	Mitigate Malicious Access to Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.18	Mitigate Malicious Access to External Data Sources and Processing	M	Yes	
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.27	Self-Monitoring for Internal CI Data Entities: Error Management	M	Yes	
		CTI 4501/3: 6.3.4.1.40	Availability of CI Data	M	Yes	
		CTI 4501/3: 6.3.4.1.41	Mitigate Failures of Availability for CI Data	M	Yes	
		CTI 4501/3: 6.3.4.2.3	Secure Communications: Integrity	M	Yes	
		CTI 4501/3: 6.3.4.2.5	Secure Communications: Replay Protection	M	Yes	
		CTI 4501/3: 6.3.4.2.6	Secure Communications: Plausibility for Received Data	M	Yes	
		CTI 4501/3: 6.3.4.2.7	Secure Communications: CI-Internal Logical Component Authentication	M	Yes	
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.2.9	Secure Communications: Authentication of External CI Data Logical Interfaces	M	Yes	
		CTI 4501/3: 6.3.4.2.11	Secure Communications: Check Authentication for Received Data	M	Yes	
		CTI 4501/3: 6.3.4.2.12	Secure Communications: Manage Received Data for Which Checks Have Failed	M	Yes	
		CTI 4501/3: 6.3.4.2.13	Secure Communications: External Data Entities for Which Checks Have Failed	M	Yes	
		CTI 4501/3: 6.3.4.2.14	Secure Communications: Other Users of External Data Entities for Which Checks Have Failed	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.3.2	Data Sources: Recovery			M	Yes	
		CTI 4501/3: 6.3.4.1.28	Recovery from Failure for Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.29	Assurance of Recovery from Failure for Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.30	Source Assurance for Recovery from Failure for Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.31	Automated Recovery from Failure for Internal CI Data Entities is Not to Be an Attack Vector	M	Yes	
		CTI 4501/3: 6.3.4.13.1	System Recovery - Software and Configuration Backups	M	Yes	
		CTI 4501/3: 6.3.4.13.2	List of Operator-Notifiable Events	M	Yes	
		CTI 4501/3: 6.3.4.13.3	List of Systemic Failure Events	M	Yes	
		CTI 4501/3: 6.3.4.13.4	Cyber Attack Must Be Addressed	M	Yes	
		CTI 4501/3: 6.3.4.13.5	Recovery Plan from Systemic Failure	M	Yes	
		CTI 4501/3: 6.3.4.13.6	Recovery from Systemic Failure Only When Necessary	M	Yes	
		CTI 4501/3: 6.3.4.13.7	Preserve Access Control During Systemic Failure	M	Yes	
		CTI 4501/3: 6.3.4.13.8	Robustness of Recovery from Systemic Failure	M	Yes	
		CTI 4501/3: 6.3.4.13.9	Assurance of Recovery from Systemic Failure	M	Yes	
		CTI 4501/3: 6.3.4.13.10	Source Assurance for Recovery from Failure for Internal Data Sources or Processors	M	Yes	
		CTI 4501/3: 6.3.4.13.11	Automated Recovery from Failure for The CI is Not to Be an Attack Vector	M	Yes	
		CTI 4501/3: 6.3.4.13.12	Vulnerability Management for Potential Cyber Attack	M	Yes	
		CTI 4501/3: 6.3.4.13.13	Security Validation	M	Yes	
		CTI 4501/3: 6.3.4.13.16	Security Knowledge for Personnel	M	Yes	
		CTI 4501/3: 6.3.4.14.5	CPMS: Error Management	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.3.3	Data Processing: Resilience			M	Yes	
		CTI 4501/3: 6.3.4.1.15	Mitigate Malicious Access to Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.18	Mitigate Malicious Access to External Data Sources and Processing	M	Yes	
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.27	Self-Monitoring for Internal CI Data Entities: Error Management	M	Yes	
		CTI 4501/3: 6.3.4.1.40	Availability of CI Data	M	Yes	
		CTI 4501/3: 6.3.4.1.41	Mitigate Failures of Availability for CI Data	M	Yes	
		CTI 4501/3: 6.3.4.2.3	Secure Communications: Integrity	M	Yes	
		CTI 4501/3: 6.3.4.2.5	Secure Communications: Replay Protection	M	Yes	
		CTI 4501/3: 6.3.4.2.6	Secure Communications: Plausibility for Received Data	M	Yes	
		CTI 4501/3: 6.3.4.2.7	Secure Communications: CI-Internal Logical Component Authentication	M	Yes	
		CTI 4501/3: 6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	O	Yes/No	
		CTI 4501/3: 6.3.4.2.9	Secure Communications: Authentication of External CI Data Logical Interfaces	M	Yes	
		CTI 4501/3: 6.3.4.2.11	Secure Communications: Check Authentication for Received Data	M	Yes	
		CTI 4501/3: 6.3.4.2.12	Secure Communications: Manage Received Data for Which Checks Have Failed	M	Yes	
		CTI 4501/3: 6.3.4.2.13	Secure Communications: External Data Entities for Which Checks Have Failed	M	Yes	
		CTI 4501/3: 6.3.4.2.14	Secure Communications: Other Users of External Data Entities for Which Checks Have Failed	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.3.4	Data Processing: Recovery			M	Yes	
		CTI 4501/3: 6.3.4.1.28	Recovery from Failure for Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.29	Assurance of Recovery from Failure for Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.30	Source Assurance for Recovery from Failure for Internal CI Data Entities	M	Yes	
		CTI 4501/3: 6.3.4.1.31	Automated Recovery from Failure for Internal CI Data Entities is Not to Be an Attack Vector	M	Yes	
		CTI 4501/3: 6.3.4.13.1	System Recovery - Software and Configuration Backups	M	Yes	
		CTI 4501/3: 6.3.4.13.2	List of Operator-Notifiable Events	M	Yes	
		CTI 4501/3: 6.3.4.13.3	List of Systemic Failure Events	M	Yes	
		CTI 4501/3: 6.3.4.13.4	Cyber Attack Must Be Addressed	M	Yes	
		CTI 4501/3: 6.3.4.13.5	Recovery Plan from Systemic Failure	M	Yes	
		CTI 4501/3: 6.3.4.13.6	Recovery from Systemic Failure Only When Necessary	M	Yes	
		CTI 4501/3: 6.3.4.13.7	Preserve Access Control During Systemic Failure	M	Yes	
		CTI 4501/3: 6.3.4.13.8	Robustness of Recovery from Systemic Failure	M	Yes	
		CTI 4501/3: 6.3.4.13.9	Assurance of Recovery from Systemic Failure	M	Yes	
		CTI 4501/3: 6.3.4.13.10	Source Assurance for Recovery from Failure for Internal Data Sources or Processors	M	Yes	
		CTI 4501/3: 6.3.4.13.11	Automated Recovery from Failure for The CI is Not to Be an Attack Vector	M	Yes	
		CTI 4501/3: 6.3.4.13.12	Vulnerability Management for Potential Cyber Attack	M	Yes	
		CTI 4501/3: 6.3.4.13.13	Security Validation	M	Yes	
		CTI 4501/3: 6.3.4.13.16	Security Knowledge for Personnel	M	Yes	
		CTI 4501/3: 6.3.4.14.5	CPMS: Error Management	M	Yes	
5.4.4.4	Diagnostics And Reporting Security					
5.4.4.4.1	Diagnostics For Security Issues			M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26	Self-Monitoring for Internal CI Data Entities: Robustness	M	Yes	
		CTI 4501/3: 6.3.4.14.2	Events to be Monitored by the CPMS	M	Yes	
		CTI 4501/3: 6.3.4.14.3	CPMS: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.14.4	CPMS: Robustness Against Invalid Input	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.4.2	Diagnostics For Incorrect Operations			M	Yes	
		CTI 4501/3: 6.3.4.7.3	Detect Inconsistency of SPaT and Signal Timing Data	M	Yes	
		CTI 4501/3: 6.3.4.8.4	Prevent Inconsistency of MAP and Road Geometry or Use: False Positives	M	Yes	
5.4.4.4.3	Confidential Information Within Diagnostics Systems			M	Yes	
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.14.1	CI Performance Monitoring System	M	Yes	
5.4.4.4.4	Correct Information Within Diagnostics System			M	Yes	
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.26	Self-Monitoring for Internal CI Data Entities: Robustness	M	Yes	
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.14.1	CI Performance Monitoring System	M	Yes	
5.4.4.4.5	Confidential Information Within Performance Monitoring Systems					
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.14.1	CI Performance Monitoring System	M	Yes	
5.4.4.4.6	Correct Information Within Performance Monitoring Systems					
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.26	Self-Monitoring for Internal CI Data Entities: Robustness	M	Yes	
		CTI 4501/3: 6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	M	Yes	
		CTI 4501/3: 6.3.4.14.1	CI Performance Monitoring System	M	Yes	
5.4.4.5	Operations and Life Cycle					
5.4.4.5.1	Security Interoperability			M	Yes	
		CTI 4501/3: 6.3.4.15.5	Tracking Evolution Of CI-Related Standards	M	Yes	
		CTI 4501/3: 6.3.4.15.6	Tracking Of Installed Version Information To CI-Related Standards	M	Yes	
		CTI 4501/3: 6.3.4.15.7	Update Cadence of CI Systems To CI-Related Standards	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.5.2	Life Cycle Security Needs					
5.4.4.5.2.1	Security for Initial Installation			M	Yes	
		CTI 4501/3: 6.3.4.1.16	Access Control on Internal CI Data Entities During Life Cycle	M	Yes	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26	Self-Monitoring for Internal CI Data Entities: Robustness	M	Yes	
		CTI 4501/3: 6.3.4.1.27	Self-Monitoring for Internal CI Data Entities: Error Management	M	Yes	
		CTI 4501/3: 6.3.4.13.14	Access Control on Internal CI Data Entities During Life Cycle	M	Yes	
5.4.4.5.2.2	Security for Security Certificate Provisioning			M	Yes	
		CTI 4501/3: 6.3.4.1.16	Access Control on Internal CI Data Entities During Life Cycle	M	Yes	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26	Self-Monitoring for Internal CI Data Entities: Robustness	M	Yes	
		CTI 4501/3: 6.3.4.1.27	Self-Monitoring for Internal CI Data Entities: Error Management	M	Yes	
		CTI 4501/3: 6.3.4.13.14	Access Control on Internal CI Data Entities During Life Cycle	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.5.2.3	Security for Normal Operations with System Monitoring and Anomaly Detection			M	Yes	
		CTI 4501/3: 6.3.4.1.16	Access Control on Internal CI Data Entities During Life Cycle	M	Yes	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26	Self-Monitoring for Internal CI Data Entities: Robustness	M	Yes	
		CTI 4501/3: 6.3.4.1.27	Self-Monitoring for Internal CI Data Entities: Error Management	M	Yes	
		CTI 4501/3: 6.3.4.13.14	Access Control on Internal CI Data Entities During Life Cycle	M	Yes	
		CTI 4501/3: 6.3.4.13.16	Security Knowledge for Personnel	M	Yes	
5.4.4.5.2.4	Security for Maintenance/Degraded Operations			M	Yes	
		CTI 4501/3: 6.3.4.1.16	Access Control on Internal CI Data Entities During Life Cycle	M	Yes	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26	Self-Monitoring for Internal CI Data Entities: Robustness	M	Yes	
		CTI 4501/3: 6.3.4.1.27	Self-Monitoring for Internal CI Data Entities: Error Management	M	Yes	
		CTI 4501/3: 6.3.4.13.14	Access Control on Internal CI Data Entities During Life Cycle	M	Yes	
		CTI 4501/3: 6.3.4.13.16	Security Knowledge for Personnel	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.5.2.5	Security for System Outages			M	Yes	
		CTI 4501/3: 6.3.4.1.16	Access Control on Internal CI Data Entities During Life Cycle	M	Yes	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26	Self-Monitoring for Internal CI Data Entities: Robustness	M	Yes	
		CTI 4501/3: 6.3.4.1.27	Self-Monitoring for Internal CI Data Entities: Error Management	M	Yes	
		CTI 4501/3: 6.3.4.13.14	Access Control on Internal CI Data Entities During Life Cycle	M	Yes	
		CTI 4501/3: 6.3.4.13.16	Security Knowledge for Personnel	M	Yes	
5.4.4.5.2.6	Security for Equipment Upgrades/Swap-out			M	Yes	
		CTI 4501/3: 6.3.4.1.16	Access Control on Internal CI Data Entities During Life Cycle	M	Yes	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26	Self-Monitoring for Internal CI Data Entities: Robustness	M	Yes	
		CTI 4501/3: 6.3.4.1.27	Self-Monitoring for Internal CI Data Entities: Error Management	M	Yes	
		CTI 4501/3: 6.3.4.13.14	Access Control on Internal CI Data Entities During Life Cycle	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.5.2.7	Security for Software/Firmware Updates			M	Yes	
		CTI 4501/3: 6.3.4.1.16	Access Control on Internal CI Data Entities During Life Cycle	M	Yes	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26	Self-Monitoring for Internal CI Data Entities: Robustness	M	Yes	
		CTI 4501/3: 6.3.4.1.27	Self-Monitoring for Internal CI Data Entities: Error Management	M	Yes	
		CTI 4501/3: 6.3.4.13.14	Access Control on Internal CI Data Entities During Life Cycle	M	Yes	
5.4.4.5.2.8	Security for System Revalidation Following Recovery or Changes			M	Yes	
		CTI 4501/3: 6.3.4.1.16	Access Control on Internal CI Data Entities During Life Cycle	M	Yes	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26	Self-Monitoring for Internal CI Data Entities: Robustness	M	Yes	
		CTI 4501/3: 6.3.4.1.27	Self-Monitoring for Internal CI Data Entities: Error Management	M	Yes	
		CTI 4501/3: 6.3.4.13.14	Access Control on Internal CI Data Entities During Life Cycle	M	Yes	
		CTI 4501/3: 6.3.4.13.16	Security Knowledge for Personnel	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.5.2.9	Security for Equipment Removal/Decommissioning			M	Yes	
		CTI 4501/3: 6.3.4.1.16	Access Control on Internal CI Data Entities During Life Cycle	M	Yes	
		CTI 4501/3: 6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	C	Yes/No	Mandatory if a CI may use data from unauthorized CI data entities.
		CTI 4501/3: 6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	O	Yes/No	
		CTI 4501/3: 6.3.4.1.26	Self-Monitoring for Internal CI Data Entities: Robustness	M	Yes	
		CTI 4501/3: 6.3.4.1.27	Self-Monitoring for Internal CI Data Entities: Error Management	M	Yes	
		CTI 4501/3: 6.3.4.13.14	Access Control on Internal CI Data Entities During Life Cycle	M	Yes	
5.4.4.5.3	Maintenance Security Needs			M	Yes	
		CTI 4501/3: 6.3.4.13.15	Maintenance Security Needs	M	Yes	
		CTI 4501/3: 6.3.4.13.16	Security Knowledge for Personnel	M	Yes	
5.4.4.5.4	System Upgradeability Security Needs					
5.4.4.5.4.1	Upgrade System: Correct Operation			M	Yes	
		CTI 4501/3: 6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	M	Yes	
		CTI 4501/3: 6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	M	Yes	
		CTI 4501/3: 6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	M	Yes	
		CTI 4501/3: 6.3.4.1.49	CI Data Entity Update: Validation	M	Yes	
		CTI 4501/3: 6.3.4.15.1	Prevent Unauthorized CI Software and Configuration Changes	M	Yes	
		CTI 4501/3: 6.3.4.15.2	Authenticate And Verify Integrity of All Software/Firmware Updates	O	Yes/No	
		CTI 4501/3: 6.3.4.15.3	CI Data Entity Update: Validation	M	Yes	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
5.4.4.5.4.2	Upgrade System: Correct Status			M	Yes	
		CTI 4501/3: 6.3.4.1.24	Events to be Monitored by Self-Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.1.26	Self-Monitoring for Internal CI Data Entities: Robustness	M	Yes	
		CTI 4501/3: 6.3.4.1.50	CI Data Entity Update: Correct Status	M	Yes	
		CTI 4501/3: 6.3.4.15.3	CI Data Entity Update: Validation	M	Yes	
		CTI 4501/3: 6.3.4.15.4	CI Data Entity Update: Correct Status	M	Yes	
5.4.4.6	Security Performance Needs					
5.4.4.6.1	Security Performance: Size			M	Yes	
		CTI 4501/3: 6.3.4.2.22	Security Size Overhead	M	Yes	
5.4.4.6.2	Security Performance: Latency					
		CTI 4501/3: 6.3.4.2.23	Security Processing Overhead	M	Yes	
5.4.4.7	Privacy Needs			M	Yes	
		CTI 4501/3: 6.3.4.1.44	List of Privacy-Sensitive Information per CI Data Entity	M	Yes	
		CTI 4501/3: 6.3.4.1.45	Protecting Privacy-Sensitive Information per CI Data Entity	M	Yes	
5.4.5	Operations and Maintenance Needs					
5.4.5.1	Interoperability and Longevity					
		6.3.5.1.1	Mean-Time-Between-Failures (MTBF)	M	Yes	
		6.3.5.1.2	Operational Uptime	M	Yes	
		6.3.5.1.3	Continuous Operation	M	Yes	
		6.3.5.1.4	Continue to Transmit MAP Messages	M	Yes	
5.4.5.2	Life Cycle			M	Yes	
		6.3.5.2.1	Documented Plan for Life Cycle Operations & Maintenance	M	Yes	
5.4.5.3	Maintenance			M	Yes	
		6.3.5.3.1	Support Normal Mode	M	Yes	
		6.3.5.3.2	Maintenance Mode	M	Yes	
		6.3.5.3.3	Report Operational Mode Status	M	Yes	
		6.3.5.3.4	Support Maintenance Mode Fallback	M	Yes	
		6.3.5.3.5	Perform Validation	M	Yes	
		6.3.5.3.6	Command Maintenance Mode	M	Yes	
		6.3.5.3.7	Automatic Return to Normal Mode	O	Yes/No	

Needs to Requirements Traceability Matrix (NRTM)						
User Need ID	**User Need**	**FR ID**	**Functional Requirement**	**Conformance**	**Support**	**Additional Specifications**
		CTI 4501/3: 6.3.4.16.1	Correct Operational Mode Protection	M	Yes	
		CTI 4501/3: 6.3.4.16.2	Correct Mode and Status Reporting	M	Yes	
		CTI 4501/3: 6.3.4.16.3	Protection Against Improper Operation in Maintenance Mode	M	Yes	
		CTI 4501/3: 6.3.4.16.4	Protecting Determinations That Normal Mode Transition Criteria Are Met	M	Yes	
		CTI 4501/3: 6.3.4.16.5	Correct Representation of Operating Mode	M	Yes	
5.4.5.4	System Diagnostic			M	Yes	
		6.3.5.4.1	System Malfunction Alert	M	Yes	
		6.3.5.4.2	Detect System Exceptions	M	Yes	
		6.3.5.4.3	System Exception Reporting	M	Yes	
		6.3.5.4.4	System Component Diagnostics	M	Yes	
5.4.5.5	System Performance Monitoring			M	Yes	
		6.3.5.5.1	Support Monitoring System	M	Yes	
		6.3.5.5.2	Support Maintenance Mode in Monitoring	M	Yes	
		CTI 4501/3: 6.3.4.16.1	Correct Operational Mode Protection	M	Yes	
		CTI 4501/3: 6.3.4.16.3	Protection Against Improper Operation in Maintenance Mode	M	Yes	
		CTI 4501/3: 6.3.4.16.4	Protecting Determinations That Normal Mode Transition Criteria Are Met	M	Yes	
5.4.5.6	System Upgradeability			M	Yes	
		6.3.5.6.1	Support Software Updates	M	Yes	
5.4.5.7	System Recovery			M	Yes	
		6.3.5.7.1	Support Operational Mode Following Recovery	M	Yes	
		6.3.5.7.2	Device Power Interruption Recovery	M	Yes	
		6.3.5.7.3	Restore Communications Automatically	M	Yes	
		6.3.5.7.4	Process Recovery	M	Yes	
5.4.5.8	Self-Correcting Operation			M	Yes	
		6.3.5.1.3	Continuous Operation	M	Yes	
		6.3.5.3.3	Report Operational Mode Status	M	Yes	
		6.3.5.4.2	Detect System Exceptions	M	Yes	
		6.3.5.4.3	System Exception Reporting	M	Yes	

6.3 Requirements

The requirements for CTI 4501 follow.

6.3.1 Architectural Requirements

The requirements for wireless communications from a connected intersection to the applications on an OBU/MU follow.

6.3.1.1 LTE-V2X Communications Parameters

A connected intersection shall exchange data with OBUs/MUs using LTE-V2X Communication, as specified in SAE J3161.

NOTE: The use of Semi-Persistent Scheduling (SPS) and/or one-shot transmissions is not specified in CTI 4501 and can be configured automatically by the RSU if the minimum packet delay budget (PDB) requirement for the corresponding traffic class is met.

6.3.1.1.1 Traffic Class Requirements

When using LTE-V2X, each packet generated by the application layer is associated with a priority value, called ProSe per packet priority (PPPP). PPPP can be used to determine the PDB, Channel Occupancy Ratio (CR) limit, and Reference Signal Receive Power (RSRP) threshold for accessing the channel. The requirements for PPPP for transmitted messages follow.

Refer to SAE J3161 for the definition of and background on SPS and one-shot transmission, PPPP, and PDB.

6.3.1.1.1.1 ProSe Per Packet Priority - SPaT Message

Refer to CTI 4501/1, 6.3.1.1.1.1, ProSe Per Packet Priority - SPaT Message.

6.3.1.1.1.2 ProSe Per Packet Priority - MAP Message

Refer to CTI 4501/2, 6.3.1.1.1.2, ProSe Per Packet Priority - MAP Message.

6.3.1.1.1.3 ProSe Per Packet Priority - RTCMcorrections Message

Refer to SAE J3258, 6.1, LTE-V2X Settings.

6.3.1.1.2 Transmit Radio Requirements

The transmit radio requirements for wireless communications using LTE-V2X from a connected intersection to the applications on an OBU/MU follow.

6.3.1.1.2.1 Transmit Radio - SPaT Message

Refer to CTI 4501/1, 6.3.1.1.2.1, Transmit Radio - SPaT Message.

6.3.1.1.2.2 Transmit Radio - MAP Message

Refer to CTI 4501/2, 6.3.1.1.2.2, Transmit Radio - MAP Message.

6.3.1.1.2.3 Transmit Radio - RTCMcorrectionsMessage

Refer to SAE J3258, Appendix B, LTE-V2X Configuration.

6.3.2 TSC Infrastructure to RSU Requirements

Refer to CTI 4501/1, 6.3.2, TSC Infrastructure to RSU Requirements.

6.3.3 Message Requirements

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

6.3.3.1 Message Performance Requirements

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

6.3.3.1.1 Uniform Message Requirements

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

NOTE: Required Data Elements are defined as optional in SAE J2735 but necessary to fulfill the CI requirements as indicated in the NRTM.

6.3.3.1.1.1 SPaT Message - SAE J2735

Refer to CTI 4501/1, 6.3.3.1.1.1, SPaT Message - SAE J2735.

6.3.3.1.1.2 SPaT Message - Mandatory Data Elements

Refer to CTI 4501/1, 6.3.3.1.1.2, SPaT Message - Mandatory Data Elements.

6.3.3.1.1.3 SPaT Message - Required Data Elements

Refer to CTI 4501/1, 6.3.3.1.1.3, SPaT Message - Required Data Elements.

6.3.3.1.1.4 SPaT Message PSID

Refer to CTI 4501/1, 6.3.3.1.1.4, SPaT Message PSID.

6.3.3.1.1.5 MAP Message - SAE J2735

Refer to CTI 4501/2, 6.3.3.1.1.5, MAP Message - SAE J2735.

6.3.3.1.1.6 MAP Message - Mandatory Data Elements

Refer to CTI 4501/2, 6.3.3.1.1.6, MAP Message - Mandatory Data Elements.

6.3.3.1.1.7 MAP Message - Required Data Elements

Refer to CTI 4501/2, 6.3.3.1.1.7, MAP Message - Required Data Elements.

6.3.3.1.1.8 MAP Message PSID

Refer to CTI 4501/2, 6.3.3.1.1.8, MAP Message PSID.

6.3.3.1.1.9 RTCMcorrections Message - SAE J2735

Refer to SAE J3258, 6.2.1, RTCMcorrections Message - SAE J2735.

6.3.3.1.1.10 RTCMcorrections Message - Mandatory Data Elements

Refer to SAE J3258, 6.2.2, RTCMcorrections Message - Mandatory Data Elements.

6.3.3.1.1.11 RTCMcorrections Message - Required Data Elements

Refer to SAE J3258, 6.2.3, RTCMcorrections Message - Required Data Elements.

6.3.3.1.1.12 RTCMcorrections Message PSID

Refer to SAE J3258, 6.2.4, RTCMcorrections Message PSID.

6.3.3.1.1.13 BSM Message - SAE J2735

Refer to CTI 4501/1, 6.3.3.1.1.13, BSM Message - SAE J2735.

6.3.3.1.1.14 BSM Message PSID

Refer to CTI 4501/1, 6.3.3.1.1.14, BSM Message PSID.

6.3.3.1.2 Robustness Requirements

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

6.3.3.1.2.1 Broadcast SPaT Message

Refer to CTI 4501/1, 6.3.3.1.2.1, Broadcast SPaT Message.

6.3.3.1.2.2 Continuous Broadcast of SPaT Messages

Refer to CTI 4501/1, 6.3.3.1.2.2, Continuous Broadcast of SPaT Messages.

6.3.3.1.3 Concise Messages Requirements

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

6.3.3.1.3.1 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.

6.3.3.1.3.2 Concise MAP Message Requirements

Refer to CTI 4501/2, 6.3.3.1.3.2, Concise MAP Message Requirements.

6.3.3.1.4 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.

6.3.3.1.4.1 Data Coverage - Every Ingress Lane

A connected intersection shall broadcast messages such that the messages can be received by OBUs/MUs in each lane approaching the intersection within the range of the ingress lane as identified in 6.3.3.1.4.2, Advanced Notification - Time. The requirement applies to SPaT, MAP, and RTCMcorrections messages.

6.3.3.1.4.2 Advanced Notification - Time

A connected intersection shall broadcast messages to a distance of at least 10 seconds at the approach speed before approaching vehicles reach the stop line on all approaches.

See 7.3.3.1.4.2, Advanced Notification - Time Guidance, for additional details.

NOTE: A value of 10 seconds was selected based on past research and experience, which considered OBU processing latency, driver reaction time, and stopping distance, and reflect the needs of the OBU of a passenger vehicle to support a RLVW application. This value may change in future revisions of this report if further studies show a different value is more appropriate.

6.3.3.1.5 Timeliness Requirements

The requirements for indicating changes in the signal indication state and timing follow.

6.3.3.1.5.1 SPaT Message - Broadcast Latency and Accuracy

Refer to CTI 4501/1, 6.3.3.1.5.1, SPaT Message - Broadcast Latency and Accuracy.

6.3.3.1.5.2 SPaT Message - Broadcast Periodicity

Refer to CTI 4501/1, 6.3.3.1.5.2, SPaT Message - Broadcast Periodicity.

6.3.3.1.5.3 MAP Message - Broadcast Periodicity

Refer to CTI 4501/2, 6.3.3.1.5.3, MAP Message - Broadcast Periodicity.

6.3.3.1.6 Quality Assurance Requirements

The requirements to provide quality information follow.

6.3.3.1.6.1 Completeness - SPaT Message

Refer to CTI 4501/1, 6.3.3.1.6.1, Completeness - SPaT Message.

6.3.3.1.6.2 Completeness - MAP Message

Refer to CTI 4501/2, 6.3.3.1.6.2, Completeness - MAP Message.

6.3.3.1.6.3 SPaT Message - Time Mark Accuracy

Refer to CTI 4501/1, 6.3.3.1.6.3, SPaT Message - Time Mark Accuracy.

6.3.3.2 Generic Message Requirements

The requirements for a connected intersection transmitting data follow.

6.3.3.2.1 Time Accuracy

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

6.3.3.2.2 Message Revision Requirements

The requirements for messages that have changed since the previous transmission follow.

6.3.3.2.2.1 SPaT Message - Revision Counter Increment

Refer to CTI 4501/1, 6.3.3.2.2.1, SPaT Message - Revision Counter Increment.

6.3.3.2.2.2 SPaT Message - Revision Counter Not Increment

Refer to CTI 4501/1, 6.3.3.2.2.2, SPaT Message - Revision Counter Not Increment.

6.3.3.2.2.3 MAP Message - Revision Counter Increment

Refer to CTI 4501/2, 6.3.3.2.2.3, MAP Message - Revision Counter Increment.

6.3.3.2.2.4 MAP Message - Revision Counter Not Increment

Refer to CTI 4501/2, 6.3.3.2.2.4, MAP Message - Revision Counter Not Increment.

6.3.3.2.2.5 MAP Message - Intersection Revision Counter Increment

Refer to CTI 4501/2, 6.3.3.2.2.5, MAP Message - Intersection Revision Counter Increment.

6.3.3.2.2.6 MAP Message - Intersection Revision Counter Not Increment

Refer to CTI 4501/2, 6.3.3.2.2.6, MAP Message - Intersection Revision Counter Not Increment.

6.3.3.2.2.7 RTCMcorrections Message - Sequence Number Increment

Refer to SAE J3258, 6.3.1, RTCMcorrections Message - Sequence Number Increment.

6.3.3.2.2.8 RTCMcorrections Message - Sequence Number Not Increment

Refer to SAE J3258, 6.3.2, RTCMcorrections Message - Sequence Number Not Increment.

6.3.3.2.3 Timestamp Requirements

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

6.3.3.2.3.1 SPaT Message - Message Timestamp

Refer to CTI 4501/1, 6.3.3.2.3.1, SPaT Message - Message Timestamp.

6.3.3.2.3.2 SPaT Message - Intersection Timestamp

Refer to CTI 4501/1, 6.3.3.2.3.2, SPaT Message - Intersection Timestamp.

6.3.3.3 Signal Timing Data Requirements

Refer to CTI 4501/1, 6.3.3.3, Signal Timing Data Requirements.

6.3.3.4 Roadway Geometry Data Requirements

Refer to CTI 4501/2, 6.3.3.4, Roadway Geometry Data Requirements.

6.3.3.5 Positioning Message Requirements

Refer to SAE J3258, 6.4, Positioning Messages, and SAE J3258, 6.5, RTK Source Requirements.

6.3.3.6 Vehicle Message Requirements

Refer to CTI 4501/1, 6.3.3.6, Vehicle Messages Requirements.

6.3.4 Security Requirements

Refer to CTI 4501/3, 6.3.4, Security Requirements.

6.3.5 Operations and Maintenance Requirements

The requirements supporting operational and maintenance needs for a connected intersection follow.

6.3.5.1 Interoperability Requirements

The requirements for connected intersection performance follow.

6.3.5.1.1 Mean Time Between Failures (MTBF)

The connected intersection and its component hardware shall be designed to achieve calculated MTBF of at least 100000 hours.

6.3.5.1.2 Operational Uptime

The connected intersection system functionality (i.e., implemented in software, firmware, and system configuration) shall support a minimum uptime of 1000 hours of continuous 24/7 operation in Normal Mode without human intervention.

This target corresponds to a month-long operation which is expected to be testable and far surpassed in actual system implementations. Another qualitative expectation for reliability is to have the connected intersection operate as reliably as the traffic signal controller.

These stated performance requirements are provided as guidance toward achieving sustained connected intersection system availability in future deployments exceeding 99.5%.

6.3.5.1.3 Continuous Operation

A connected intersection shall be designed to operate continuously 24/7 in Normal Mode (see 6.3.5.3.1, Support Normal Mode) without human intervention, unless there is a power disruption.

NOTE: A connected intersection is expected to be as reliable as a traffic signal controller.

6.3.5.1.4 Continue to Transmit MAP Messages

A connected intersection shall continue to transmit MAP messages, even if the connected intersection is broadcasting SPaT messages that are Not Valid. Refer to CTI 4501/1, 6.3.3.3.2.14, No SPaT Available.

6.3.5.2 Life Cycle Requirements

The requirements to accommodate the life cycle of a connected intersection follow.

6.3.5.2.1 Documented Plan for Life Cycle Operations & Maintenance

A connected intersection shall adhere to a documented plan aligned with the life cycle process and practices of the responsible agency (i.e., IOO) (see 5.4.5.2). The CVPFS Connected Intersection Guidance Document may be used as guidance in addition to other existing agency policies and procedures.

6.3.5.3 Maintenance Requirements

The requirements for maintaining a connected intersection follow.

6.3.5.3.1 Support Normal Mode

A connected intersection shall support a "Normal Mode." In the Normal Mode, the connected intersection operates with full capabilities, broadcasting SPaT, MAP, and RTCMcorrections messages, compliant to all mandatory requirements specified in this document. All individual components (e.g., RSU, TSC Infrastructure) must operate normally in the Normal Mode.

6.3.5.3.2 Maintenance Mode

A connected intersection shall support a Maintenance Mode. The Maintenance Mode can be utilized for system updates or when an anomaly preventing normal operation is detected. In the Maintenance Mode, the connected intersection may do the following:

- Stop broadcasting any messages.
- Omit some of the required messages, e.g., SPaT message, MAP message, or RTCMcorrections message. However, if SPaT messages are transmitted, they must indicate that the connected intersection is operating in Maintenance Mode.
- Transmit all required message types (i.e., SPaT, MAP, RTCMcorrections) and include the IntersectionStatus object indicating that the messages are not suitable for end-user applications.

The connected intersection is defined to be in Maintenance Mode if any of the following is true:

- The failureFlash (2) bit in the IntersectionStatus object is enabled.
- The failureMode (8) bit in the IntersectionStatus object is enabled.
- The off (9) bit in the IntersectionStatus object is enabled.
- The noValidMAPisAvailableAtThisTime (12) bit in the IntersectionStatus object is enabled.
- The noValidSPATisAvailableAtThisTime (13) bit in the IntersectionStatus object is enabled.
- The SPaT message is not signed with the appropriate security certificates.

A connected intersection may support additional modes of operation, transmitting some other messages which may be suitable for other applications other than those described in CTI 4501. Definitions of these modes and detailed operations of the CI system supporting these applications are outside the scope of this document.

NOTE: The RSU may have a "Standby Mode" where the RSU does not transmit any messages.

6.3.5.3.3 Report Operational Mode Status

A connected intersection shall report the running (Normal, Maintenance) mode of the connected intersection and the operational status of its individual component (e.g., RSU, TSC Infrastructure) to a CPMS and be accessible for an authorized operator.

6.3.5.3.4 Support Maintenance Mode Fallback

A connected intersection shall automatically transition to the Maintenance mode if any individual CI component (e.g., RSU, TSC Infrastructure) causes an anomaly that renders the connected intersection non-compliant to this specification (see 6.3.5.3.1 for a definition of Normal Mode).

The running mode of the connected intersection represents its overall system functionality. While individual components may still support Normal Mode, if any component or a combination of components causes omission of any required message (i.e., SPaT, MAP, RTCMcorrections) or the messages or their contents are not compliant to this specification, then the connected intersection must transition into the Maintenance mode.

6.3.5.3.5 Perform Validation

A connected intersection shall perform and pass validation tests before transitioning from Maintenance into Normal Mode. The validation tests are based on predefined and documented criterion following the IOO's adopted validation process. The validation tests may be initiated automatically based on predefined and documented rules. The IOO's validation criterion can refer to test specifications and reports such as CTI 4501, CTI 4502, SAE J3238/1, SAE J3238/2, and SAE J3258.

All software/firmware updates to CI components shall be conducted in Maintenance mode. After software/firmware updates are complete, a predefined set of regression validation tests shall be performed before entering Normal mode and resuming normal operation. Refer to CTI 4501/4, B.2.4.2.4, CI - Operations and Maintenance.

6.3.5.3.6 Command Maintenance Mode

A connected intersection shall allow an authorized operator to command the connected intersection to Maintenance Mode operation. This allows an IOO to suspend transmission of messages that may be unusable for the end-user applications during the maintenance period.

6.3.5.3.7 Automatic Return to Normal Mode

A connected intersection shall automatically switch from Maintenance Mode to Normal Mode if all predefined and documented rules are fulfilled.

6.3.5.4 System Diagnostic Interface Requirements

The requirements for a connected intersection's diagnostic interface follow.

6.3.5.4.1 System Malfunction Alert

Each CI component (e.g., RSU, TSC Infrastructure) shall monitor its own health and detect critical failures. Critical failures are those which preclude the connected intersection from operating in Normal Mode.

6.3.5.4.2 Detect System Exceptions

CI components (one or several) shall be able to detect the following system exceptions, where each condition must be detected and reported by at least one CI component:

- Loss of network connection between the CPMS to any other CI component.
- Loss of power to any individual components in excess of thresholds (specific value to be selected by an IOO). Note that NEMA and ATC controllers may sustain their functionality during power interruptions up to 0.5 second. Some traffic cabinets may have battery backups. Detecting power interruptions can help to improve CI system availability over time.
- Loss of or irregularity in SPaT, MAP, or RTCMcorrections message broadcasts with thresholds specified in SAE J3238/1, SAE J3238/2, and SAE J3258.
- Loss of validity for messaging signing security certificates.
- Inconsistency of SPaT data with equivalent messages sent over the TSC serial bus for activation of the physical signal heads exceeding the 250 ms latency (see 6.3.3.1.5.4).

The list may be expanded to include critical failures specific to each component.

6.3.5.4.3 System Exception Reporting

The detected system exceptions shall be reported to the CPMS and available for viewing and response by an authorized operator.

6.3.5.4.4 System Component Diagnostics

A CPMS shall send diagnostic logs and reports to authorized operators when a component (e.g., RSU, TSC Infrastructure) malfunctions. The logs and reports are used to help diagnose and rectify malfunctions.

6.3.5.5 CPMS Requirements

The requirements for monitoring the system performance of a connected intersection follow.

6.3.5.5.1 Support Monitoring System

A CPMS shall monitor a connected intersection's compliance to the relevant (all mandatory and implemented optional) requirements in CTI 4501. The monitoring system is expected to implement a minimum scope comparable to that described in the CVPFS CIMMS Systems Requirements for the following conditions:

- Detect inconsistencies between SPaT/MAP/RTCM data and CTI 4501 message requirements (e.g., omission of required data elements).
- Detect inconsistencies between SPaT and MAP data elements (e.g., signal group and lane assignments).
- Detect interruptions in message outputs from an RSU (e.g., omission of SPaT, MAP, or RTCMcorrections messages).
- Detect inconsistencies between the broadcasted MAP message and physical intersection layout (e.g., using BSMs).
- Use BSMs to detect inconsistencies between the broadcasted SPaT messages and traffic signal controller phase and timing information.
- Monitor use of IEEE Std 1609.2 security signatures, validity of security certificates, and for security misbehavior.

Detected inconsistencies affecting connected intersection operation in Normal Mode shall be translated into system exceptions reported to the CPMS.

6.3.5.5.2 Support Maintenance Mode in Monitoring

A connected intersection shall be placed into Maintenance Mode when performance deviates from the agency's documented expected performance requirements. See 6.3.5.3.2.

6.3.5.6 System Upgradeability Requirements

The requirements for connected intersection system upgradeability follow.

6.3.5.6.1 Support Software Updates

All individual components of a connected intersection (e.g., RSU, TSC Infrastructure) shall support software updates and configuration changes locally and remotely by authorized personnel. This requirement is intended to ensure that this capability is available in all CI components (i.e., RSU, TSC Infrastructure).

For an RSU, this feature is defined in CTI 4001, 2.5.1.14, Software and Firmware Updates. Similar features are expected for a TSC Infrastructure.

6.3.5.7 System Recovery Requirements

The requirements for the system recovery of a connected intersection follow.

6.3.5.7.1 Support Operational Mode Following Recovery

A connected intersection shall be capable of recovering from significant disruptions, including power outages, network interruptions, loss of system time synchronization, and firmware updates in a consistent and repeatable manner.

This requirement supports the CI's transition to Normal Mode only when all individual components (e.g., RSU, TSC Infrastructure) have recovered from disruptions, regardless of sequence of power interruptions or sensitivity and recovery characteristics of individual components.

6.3.5.7.2 Device Power Interruption Recovery

A connected intersection shall support an automatic recovery from power interruptions for all devices at the connected intersection, including TSC Infrastructure, RSU, Video Analytics, Routers, and Switches, i.e., it needs to withstand interruptions and outages of its individual components "gracefully."

Devices are expected to automatically recover individually, as groups, and as a system. A TSC is expected to react to power interruptions as described in their applicable standards.

a. For NEMA TS 2 Controllers, refer to NEMA TS 2 Section 3.12, Power Interruption.

b. For ATC Controllers, refer to ATC 5201 Section 4.4.1, Power, and Section 5.6.5.1, Power Down and Power Up.

c. For ATC Cabinets, refer to ATC 5301 Section 6.4.

Note that the TSC has a 0.5 second power interruption requirement, but those requirements do not apply to other components in the traffic cabinet.

6.3.5.7.3 Restore Communications Automatically

A connected intersection component shall automatically restore (without operator intervention) normal communications and data exchanges with other CI components within 60 seconds after the end of any disruption. Disruption may include power disruptions or loss of communications. This time is chosen as a worst case to allow CI components to restart and acquire a GNSS reference position and time, if applicable.

NOTE: Resuming communications with the CPMS might take longer time depending on where the power outage occurs. A time threshold for reestablishing connection between a connected intersection and the CPMS to resume Normal operation will be determined by operating rules of the IOO.

6.3.5.7.4 Process Recovery

All individual components in a connected intersection shall monitor their internal processes and automatically restart failed processes to restore normal operation.

Some noted constraints to this requirement include a tripped conflict monitor (e.g., watchdog or serial bus failure) at a signalized intersection, which triggers an Exception Flash that requires manual intervention in the traffic cabinet. However, non-critical processes, such as the loss of management center communications, may be restarted without consequences to the intersection CI traffic operation.

In addition, certain individual components may monitor other components to identify the loss or failure of another component and report exceptions to the CPMS.

7. SYSTEM DESIGN

This section defines the system design details based on the requirements identified in Section 6. This section includes the following:

a. A tutorial

b. A Requirements Traceability Matrix (RTM). The RTM links the requirements presented in 6.3 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 7 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 these readers, Section 7 is useful to understand how particular functions and information may be implemented to conform to CTI 4501.

7.1 Tutorial

The Requirements Traceability Matrix (RTM) in 7.2 identifies the design details that fulfills each of the requirements defined in 6.3. 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 7.3.

7.2 Requirements Traceability Matrix

The Requirements Traceability Matrix (RTM) in Table 6 links the requirements in 6.3 with the corresponding design details on the same line. Using this table, each requirement in 6.3 can thus be traced in a conformant way. Each requirement either points to 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 are contained within the normative reference.

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

7.2.1 Notation [Informative]

7.2.1.1 Functional Requirement Columns

The functional requirements are specified within 6.3 and the RTM is based upon the requirements within that section. The section number and the functional requirement name are indicated within these columns.

7.2.1.2 Design Details

The "Design Details" column either provides a hyperlinked reference to a section number where the design details are defined within 7.3, 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).

7.2.1.3 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.

7.2.2 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 document describing how the requirement is to be fulfilled; point to a normative reference describing how to fulfill the functional requirement; or indicate "No Further Design Details" because no additional design information is necessary. The "Additional Specifications" column provides additional notes or details about the design content.

Table 6 - Requirements traceability matrix

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
6.3	Requirements		
6.3.1	Architectural Requirements		
6.3.1.1	LTE-V2X Traffic Class Settings	Refer to SAE J3161	
6.3.1.1.1	Traffic Classes Requirements		
6.3.1.1.1.1	ProSe Per Packet Priority - SPaT Message	Refer to SAE J3161	
6.3.1.1.1.2	ProSe Per Packet Priority - MAP Message	Refer to SAE J3161	
6.3.1.1.1.3	ProSe Per Packet Priority - RTCMcorrections Message	Refer to SAE J3161	
6.3.2	TSC Infrastructure to RSU Requirements		
		Refer to CTI 4501/1 Requirements Traceability Matrix	
6.3.3	Message Requirements		
6.3.3.1	Message Performance Requirements		
6.3.3.1.1	Uniform Message Requirements		
6.3.3.1.1.1	SPaT Message - SAE J2735	Refer to CTI 4501/1 Requirements Traceability Matrix	
6.3.3.1.1.2	SPaT Message - Mandatory Data Elements	Refer to CTI 4501/1 Requirements Traceability Matrix	
6.3.3.1.1.3	SPaT Message - Required Data Elements	Refer to CTI 4501/1 Requirements Traceability Matrix	
6.3.3.1.1.4	SPaT Message PSID	Refer to CTI 4501/1 Requirements Traceability Matrix	
6.3.3.1.1.5	MAP Message - SAE J2735	Refer to CTI 4501/2 Requirements Traceability Matrix	
6.3.3.1.1.6	MAP Message - Mandatory Data Elements	Refer to CTI 4501/2 Requirements Traceability Matrix	
6.3.3.1.1.7	MAP Message - Required Data Elements	Refer to CTI 4501/2 Requirements Traceability Matrix	
6.3.3.1.1.8	MAP Message PSID	Refer to CTI 4501/2 Requirements Traceability Matrix	
6.3.3.1.1.9	RTCMcorrections Message - SAE J2735	Refer to RTCMcorrections Message - SAE J2735 in SAE J3258 Requirements Traceability Matrix	
6.3.3.1.1.10	RTCMcorrections Message - Mandatory Data Elements	Refer to RTCMcorrections Message - Mandatory Data Elements in SAE J3258 Requirements Traceability Matrix	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
6.3.3.1.1.11	RTCMcorrections Message - Required Data Elements	Refer to RTCMcorrections Message - Required Data Elements in SAE J3258 Requirements Traceability Matrix	
6.3.3.1.1.12	RTCMcorrections Message PSID	Refer to RTCMcorrections Message PSID in SAE J3258 Requirements Traceability Matrix	
6.3.3.1.1.13	BSM Message - SAE J2735	Refer to CTI 4501/1 Requirements Traceability Matrix	
6.3.3.1.1.14	BSM Message PSID	Refer to CTI 4501/1 Requirements Traceability Matrix	
6.3.3.1.2	Robustness Requirements		
6.3.3.1.2.1	Broadcast SPaT Message	Refer to CTI 4501/1 Requirements Traceability Matrix	
6.3.3.1.2.2	Continuous Broadcast of SPaT Messages	Refer to CTI 4501/1 Requirements Traceability Matrix	
6.3.3.1.3	Concise Messages Requirements		
6.3.3.1.3.1	Transport Message Size - WAVE	See 7.3.3.1.3.1, Transport Message Size - WAVE	
6.3.3.1.3.2	Concise MAP Message Requirements		
		Refer to CTI 4501/2 Requirements Traceability Matrix	
6.3.3.1.4	Advanced Notification Requirements		
6.3.3.1.4.1	Data Coverage - Every Ingress Lane	See 7.3.3.1.4.1, Data Coverage - Every Lane	
6.3.3.1.4.2	Advanced Notification - Time	See 7.3.3.1.4.2, Advanced Notification - Time	
6.3.3.1.5	Timeliness Requirements		
6.3.3.1.5.1	SPaT Message - Broadcast Latency and Accuracy	Refer to CTI 4501/1 Requirements Traceability Matrix	
6.3.3.1.5.2	SPaT Message - Broadcast Periodicity	Refer to CTI 4501/1 Requirements Traceability Matrix	
6.3.3.1.5.3	MAP Message - Broadcast Periodicity	Refer to CTI 4501/2 Requirements Traceability Matrix	
6.3.3.1.6	Quality Assurance Requirements		
6.3.3.1.6.1	Completeness - SPaT Message	Refer to CTI 4501/1 Requirements Traceability Matrix	
6.3.3.1.6.2	Completeness - MAP Message	Refer to CTI 4501/2 Requirements Traceability Matrix	
6.3.3.1.6.3	SPaT Message - Time Mark Accuracy	Refer to CTI 4501/1 Requirements Traceability Matrix	
6.3.3.2	Generic Message Requirements		
6.3.3.2.1	Time Accuracy	See 7.3.3.2.1, Time Accuracy	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
6.3.3.2.2	Message Revision Requirements		
6.3.3.2.2.1	SPaT Message - Revision Counter Increment	Refer to CTI 4501/1 Requirements Traceability Matrix	
6.3.3.2.2.2	SPaT Message - Revision Counter Not Increment	Refer to CTI 4501/1 Requirements Traceability Matrix	
6.3.3.2.2.3	MAP Message - Revision Counter Increment	Refer to CTI 4501/2 Requirements Traceability Matrix	
6.3.3.2.2.4	MAP Message - Revision Counter Not Increment	Refer to CTI 4501/2 Requirements Traceability Matrix	
6.3.3.2.2.5	MAP Message - Intersection Revision Counter Increment	Refer to CTI 4501/2 Requirements Traceability Matrix	
6.3.3.2.2.6	MAP Message - Intersection Revision Counter Not Increment	Refer to CTI 4501/2 Requirements Traceability Matrix	
6.3.3.2.2.7	RTCMcorrections Message - Sequence Number Increment	Refer to RTCMcorrections Message - Sequence Number Increment in SAE J3258 Requirements Traceability Matrix	
6.3.3.2.2.8	RTCMcorrections Message - Sequence Number Not Increment	Refer to RTCMcorrections Message - Sequence Number Not Increment in SAE J3258 Requirements Traceability Matrix	
6.3.3.2.3	Timestamp Requirements		
6.3.3.2.3.1	SPaT Message - Message Timestamp	Refer to CTI 4501/1 Requirements Traceability Matrix	
6.3.3.2.3.2	SPaT Message - Intersection Timestamp	Refer to CTI 4501/1 Requirements Traceability Matrix	
6.3.3.3	Signal Timing Data Requirements		
		Refer to CTI 4501/1 Requirements Traceability Matrix	
6.3.3.4	Roadway Geometry Data Requirements		
		Refer to CTI 4501/2 Requirements Traceability Matrix	
6.3.3.5	Positioning Message Requirements		
		Refer to SAE J3258 Requirements Traceability Matrix	
6.3.3.6	Vehicle Message Requirements		
		Refer to CTI 4501/1 Requirements Traceability Matrix	
6.3.4	Security Requirements		
		Refer to CTI 4501/3 Requirements Traceability Matrix	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
6.3.5	Operations and Maintenance Requirements		
6.3.5.1	Interoperability Requirements		
6.3.5.1.1	Mean-Time-Between-Failures (MTBF)	No additional design details	
6.3.5.1.2	Operational Uptime	No additional design details	
6.3.5.1.3	Continuous Operation	No additional design details	
6.3.5.1.4	Continue to Transmit MAP Messages	No additional design details	
6.3.5.2	Life Cycle Requirements		
6.3.5.2.1	Documented Plan for Life Cycle Operations & Maintenance	No additional design details	
6.3.5.3	Maintenance Requirements		
6.3.5.3.1	Support Normal Mode	No additional design details	
6.3.5.3.2	Maintenance Mode	No additional design details	
6.3.5.3.3	Report Operational Mode Status	No additional design details	
6.3.5.3.4	Support Maintenance Mode Fallback	No additional design details	
6.3.5.3.5	Perform Validation	No additional design details	
6.3.5.3.6	Command Maintenance Mode	No additional design details	
6.3.5.3.7	Automatic Return to Normal Mode	No additional design details	
6.3.5.4	System Diagnostic Interface Requirements		
6.3.5.4.1	System Malfunction Alert	No additional design details	
6.3.5.4.2	Detect System Exceptions	No additional design details	
6.3.5.4.3	System Exception Reporting	No additional design details	
6.3.5.4.4	System Component Diagnostics	No additional design details	
6.3.5.5	CPMS Requirements		
6.3.5.5.1	Support Monitoring System	No additional design details	
6.3.5.5.2	Support Maintenance Mode in Monitoring	No additional design details	
6.3.5.6	System Upgradeability Requirements	No additional design details	
6.3.5.6.1	Support Software Updates	No additional design details	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
6.3.5.7	System Recovery Requirements		
6.3.5.7.1	Support Operational Mode Following Recovery	No additional design details	
6.3.5.7.2	Device Power Interruption Recovery	No additional design details	
6.3.5.7.3	Restore Communications Automatically	No additional design details	
6.3.5.7.4	Process Recovery	No additional design details	

7.3 Design Details

The design details to fulfill the requirements specified in 6.3 follow.

7.3.1 Architectural Design Details

The design details to fulfill the architectural requirements specified in 6.3.1 follow.

7.3.1.1 LTE-V2X Traffic Class Settings Design Details

The design details to fulfill the requirements for a connected intersection to exchange data with OBUs/MUs using LTE-V2X communications are specified in SAE J3161.

7.3.2 TSC Infrastructure to RSU Design Details

Refer to the RTM in CTI 4501/1 for the design guidance to fulfill the TSC Infrastructure to RSU Requirements.

7.3.3 Message Design Details

The design details to fulfill the requirements for a connected intersection broadcasting messages to OBUs/MUs follow. These requirements are specified in 6.3.3.

7.3.3.1 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 specified in 6.3.3.1.

7.3.3.1.1 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 are found in other documents. These requirements are specified in 6.3.3.1.1. For each requirement, see Table 6 to determine the document in which the design details can be found.

7.3.3.1.2 Robustness Design Details

The design details to fulfill the requirements for a connected intersection to operate under different degraded conditions are found in other documents. These requirements are specified in 6.3.3.1.2. For each requirement, see Table 6 to determine the document in which the design details can be found.

7.3.3.1.3 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 specified in 6.3.3.1.3.

7.3.3.1.3.1 Transport Message Size - WAVE

The default maximum transport message in IEEE Std 1609.3 for a WAVE Short Message (WSM) payload is 1400 bytes; however, a maximum of 2302 bytes is supported. 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 LTE-V2X, refer to SAE J3161, Transmit SPS Reservation Size and MCS Adjusting, for the maximum transmission unit.

7.3.3.1.3.2 Concise MAP Message Design Details

The design details to fulfill the requirements for concise MAP messages are found in CTI 4501/2. These requirements are specified in 6.3.3.1.3.2. For each requirement, refer to the RTM in CTI 4501/2 to determine where the design details for each requirement can be found.

7.3.3.1.4 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 specified in 6.3.3.1.4.

7.3.3.1.4.1 Data Coverage - Every Ingress Lane Guidance

The requirement that this design detail traces to requires that an OBU/MU in any ingress lane into the intersection and within the Advanced Notification Time (see 6.3.3.1.4.2) can receive the messages broadcasted by the connected intersection. Also see the next design detail section, 7.3.3.1.4.2.

7.3.3.1.4.2 Advanced Notification - Time Guidance

This requirement is verified (tested) by demonstration.

The requirement this design detail traces to provide guidance on how far upstream should messages received by an approaching vehicle into an intersection.

The 10 seconds stated in the requirement reflect the needs of the OBU of a passenger vehicle to support a RLVW application. Whenever possible, the messages broadcasted by the connected intersection should be received by approaching vehicles at the approach speed with at least 10 seconds of vehicle travel in the ingress lane before the stop line.

To calculate the distance that reflects 10 seconds of time, the method is, in order of precedence, to use:

a. The 85th percentile speed from a speed study for that ingress lane. If the 85th percentile is not available, then;

b. The posted speed limit plus 7 mph. If no posted speed limit is available, then;

c. The statutory speed limit plus 7 mph is used. For 25 mph, this is equivalent to an ingress lane 112 m long.

This distance may be computed by multiplying the speed in mph by 4.47 (speed in mph * 1609 meters/mile * 1 hour/ 3600 seconds * 10 seconds) to determine the distance in meters.

7.3.3.1.5 Timeliness Design Details

The design details to fulfill the requirements for indicating changes in state, timing, and physical indications are found in other documents. These requirements are specified in 6.3.3.1.5. For each requirement, see Table 6 to determine the document in which the design details can be found.

7.3.3.1.6 Quality Assurance Design Details

The design details to fulfill the requirements to provide quality information are found in other documents. These requirements are specified in 6.3.3.1.6. For each requirement, see Table 6 to determine the document in which the design details can be found.

7.3.3.2 Generic Message Design Details

The design details to fulfill requirements for a connected intersection transmitting data follow. These requirements are specified in 6.3.3.2.

7.3.3.2.1 Time Accuracy

This requirement is verified by testing.

As noted in the NRTM, this requirement is applicable to SPaT and RTCMcorrections messages. It does not apply to MAP messages.

7.3.3.2.2 Message Revision Counter Design Details

The design details to fulfill the requirements to see if the data transmitted by a connected intersection are found in other documents. These requirements are specified in 6.3.3.2.2. For each requirement, see Table 6 to determine the document in which the design details can be found.

7.3.3.2.3 Timestamp Design Details

The design details to fulfill the requirements for a timestamp in messages transmitted by a connected intersection are found in other documents. These requirements are specified in 6.3.3.2.3. For each requirement, see Table 6 to determine the document in which the design details can be found.

7.3.3.3 Signal Timing Data Design Details

Refer to the RTM in CTI 4501/1 for the design guidance to fulfill the Signal Timing Data Requirements.

7.3.3.4 Roadway Geometry Data Design Details

Refer to the RTM in CTI 4501/2 for the design guidance to fulfill the Roadway Geometry Data Requirements.

7.3.3.5 Positioning Messages

Refer to the RTM in SAE J3258 for the design guidance to fulfill the Positioning Messages Requirements.

7.3.3.6 Vehicle Messages Design Details

Refer to the RTM in CTI 4501/1 for the design guidance to fulfill the Vehicle Messages Requirements.

7.3.4 Security Design Details

Refer to the RTM in CTI 4501/3 for the design guidance to fulfill the Security Requirements.

7.3.5 Operations and Maintenance Design Details

No additional design details.

8. CONNECTED INTERSECTION TESTING

Refer to CTI 4501/4 Section 8, Connected Intersection Testing.

9. NOTES

9.1 Revision Indicator

A change bar (I) located in the left margin is for the convenience of the user in locating areas where technical revisions, not editorial changes, have been made to the previous issue of this document. An (R) symbol to the left of the document title indicates a complete revision of the document, including technical revisions. Change bars and (R) are not used in original publications, nor in documents that contain editorial changes only.

ANNEX A - ADDITIONAL INFORMATION

A.1 ROAD AUTHORITY ID

Requirements related to Road Regulator Identifier (sections 3.3.3.3.1.2, 3.3.3.4.1.2) in CTI 4501 v01 are deprecated in CTI 4501 v02. As noted in Annex H.1.5 in CTI 4501 v01, at the time CTI 4501 v01 was published, 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.

The updated requirements in CTI 4501 reference the OpOrgID (Operator Organization Identifier) in the IEEE 1609.2 certificates to identify the road authority requesting the security certificates. In conjunction with the OpOrgID, the optional DE_RelativeRoadAuthorityID, and the DE_IntersectionID, each intersection is globally uniquely identified.

A.1.1 Usage

This section describes the use of OpOrgID, DE_RelativeRoadAuthorityID, and DE_IntersectionID to define the globally unique identifier for an intersection.

All broadcasted SPaT and MAP messages must identify the unique identifier of the intersection that the message (or parts of a message) is intended for. DE_IntersectionID, defined in SAE J2735, is an integer from 0 to 65535 (note: values 0 to 255 are allocated for testing purposes only). The definition of SAE J2735 DE_IntersectionID notes that the intersection identifier is unique only within the regional ID only, also known as the Road Authority Identifier (RAID). The RAID consists of OpOrgID and optionally, the DE_RelativeRoadAuthorityID.

Thus, each unique intersection identifier consists of:

<OpOrgID> + <DE_RelativeRoadAuthorityID> + <DE_IntersectionID>

where OpOrgID and DE_IntersectionID are required to be assigned. The OpOrgID must be included in the signing certificate, and the DE_IntersectionID must be included in all broadcasted SPaT and MAP messages.

Figure A1 provides an illustration of a SPaT and MAP message that contains an OpOrgID in the security certificate, but no Relative Road Authority ID information in the SPaT or MAP message and thus the resulting RAID being just the OpOrgID. It also shows the intersection ID as being what is contained in the SPaT and MAP message.

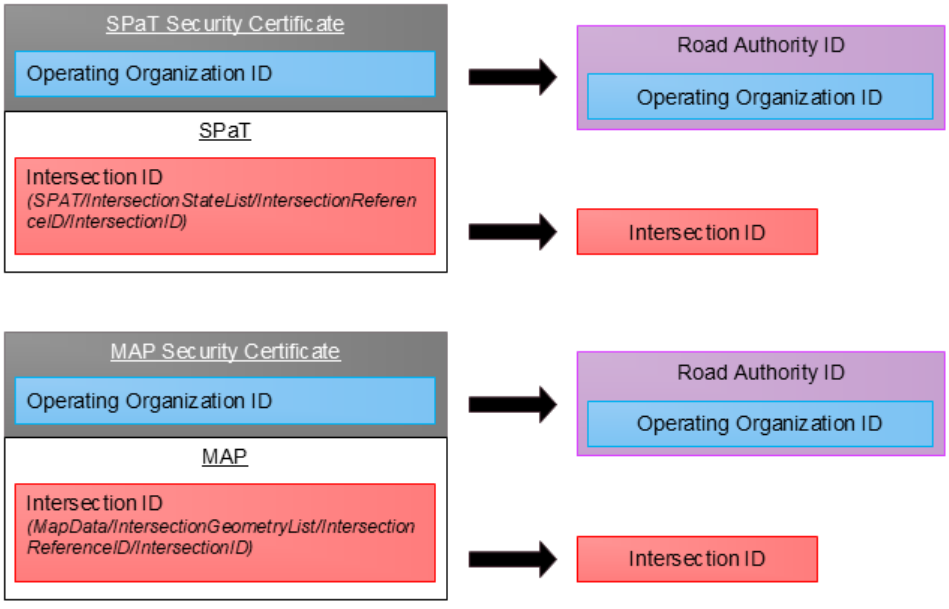


Figure A1 - SPaT/MAP intersection ID - No Relative Road Authority ID

Figure A2 provides an illustration of a SPaT and MAP message which contains an OpOrgID in the security certificate along with Relative Road Authority ID information in the SPaT and MAP messages and thus the resulting RAID being a union of the OpOrgID and the Relative Road Authority ID. It also shows the intersection ID as being what is contained in the SPaT and MAP message.

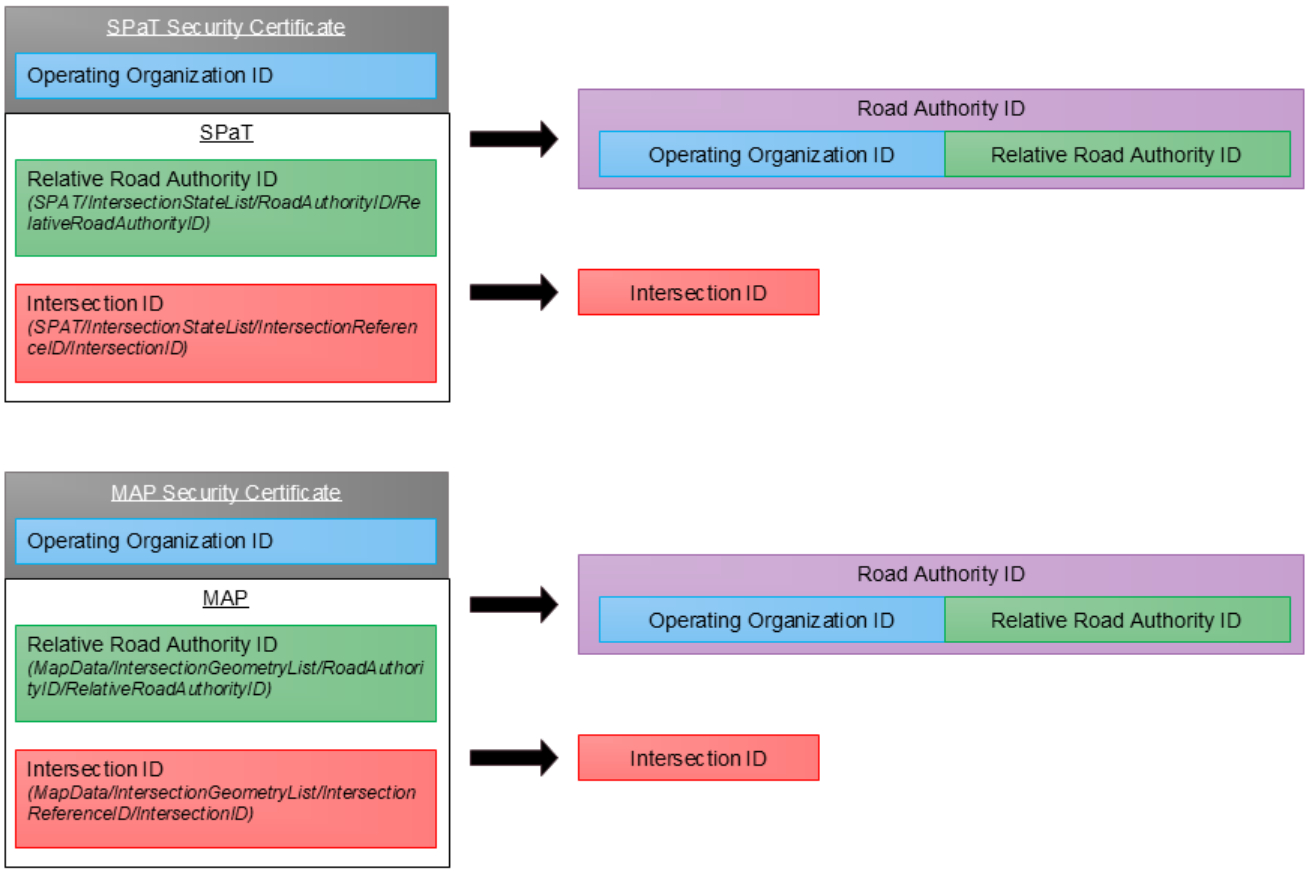


Figure A2 - SPaT/MAP intersection ID - with Relative Road Authority ID

A.1.2 OpOrgID

The Operating Organization Identifier (OpOrgID) identifies the holder of an IEEE 1609.2 certificate, called the signing certificate. To maintain security for the V2X environment, all messages broadcasted by a connected intersection must be signed, with the signing certificate issued by an SCMS provider. Each SPaT and MAP IEEE 1609.2 certificate includes the OpOrgID, which consists of an Object IDentifier (OID).

An OID corresponds to a node in the "OID tree" or hierarchy, which is formally defined using the ITU's OID standard, X.660. OIDs are often used to identify databases and objects within them by assigning specific numbers. Each node in the tree is represented by a series of integers separated by periods, corresponding to the path from the root through the series of ancestor nodes, to the node. An organization may register with the ISO registration authority for an arc. That organization then owns all sub arcs beyond its base arc.

For example, SAE "owns" the base arc – 1.3.6.1.4.1.21431, which corresponds to:

1 ISO

1.3 identified-organization (ISO/IEC 6523),

1.3.6 DoD,

1.3.6.1 internet,

1.3.6.1.4 private,

1.3.6.1.4.1 IANA enterprise numbers,

1.3.6.1.4.1.21431 SAE International

All sub arcs below 1.3.6.1.4.1.21431 are assigned by SAE International (e.g., 1.3.6.1.4.1.21431.1, 1.3.6.1.4.1.21431.2, 1.3.6.1.4.1.21431.2.x, etc.).

Each SCMS provider is expected to register for a base arc, and then assigns each certificate holder an OpOrgID (OID) under its base arc. Thus, each certificate holder organization will have a unique OpOrgID that is assigned and maintained by the SCMS provider, eliminating the need to create and maintain a registry for a Road Authority ID.

SCMS providers may offer different policy alternatives with OpOrgId assignments, such as allowing an IOO to register for its own enterprise number, thereby establishing a base arc wholly owned by the IOO. In this case, an SCMS provider can issue certificates with an OpOrgId using the IOO's base arc, provided the SCMS has verified ownership within the IANA enterprise numbers registry or another public OID registry. Lastly, different certificate holders will not have the same OpOrgId assignment. If two organizations have unique relationships with an SCMS provider, they cannot be assigned the same OpOrgId.

To search for the organizations that have registered for a base arc, go to: https://www.iana.org/assignments/enterprise-numbers/. To apply for a private enterprise number (PEN), go to: https://www.iana.org/assignments/enterprise-numbers/assignment/apply/.

Note that the OpOrgID is in the IEEE 1609.2 certificate. There is no data element defined in SAE J2735 for the exchange of the OpOrgID.

EXAMPLE:

The Department of Transportation for State A contracts with SCMS Provider C for signing certificates. SCMS Provider C has registered for an OID and is assigned 1.3.6.1.4.1.65534. SCMS Provider C then assigns an OpOrgID of 1.3.6.1.4.1.65534.51 to State A. The OpOrgID for State A is thus 1.3.6.1.4.1.65534.51.

A.1.3 Relative Road Authority Identifier

DF_RoadAuthorityID is an optional data frame defined in SAE J2735 to identify IOOs and their corresponding agencies, and divisions. DF_RoadAuthorityID is a CHOICE of either DE_FullRoadAuthorityID or DE_RelativeRoadAuthorityID. DE_RelativeRoadAuthorityID, which provides the identifier for the partially specified OID of the Road Authority, is only used when the base portion of the OID is known. Using DE_RelativeRoadAuthorityID within DF_RoadAuthorityID is always relative to the OpOrgId in the certificate, i.e., DE_RelativeRoadAuthorityID can only be used to further partition OpOrgId.

CTI 4501 guidance is to use ONLY DE_RelativeRoadAuthorityID to identify a child organization or another organization below the certificate holder. DE_FullRoadAuthorityID is not used. If there is no child organization or another organization below the certificate holder, then DE_RelativeRoadAuthorityID is omitted.

In the example above, State A is the certificate holder – meaning it has a contract with SCMS Provider C to provide signing certificates for State A. However, State A may be comprised of eight regions, and State A may decide to identify a subset of roadside units by regions – perhaps to allow each region to assign a unique DE_IntersectionID. In addition, State A also may decide to allow cities and other transportation agencies within the state to use their contract with SCMS Provider C to issue signing certificates for their roadside units. This agreement among State A, cities, and other transportation agencies to use State A's contract for signing certificates result with several economic benefits for all agencies involved. To allow each region, city, and transportation agency to assign and maintain their own unique intersection identifiers, State A assigns unique relative road authority identifiers, i.e., DE_RelativeRoadAuthorityID, for each region, city, and transportation agency.

Using the example above,

- State A assigns Region 1 in State A an OID of 1.3.6.1.4.1.65534.51.1, Region 2 an OID of 1.3.6.1.4.1.65534.51.2, etc.
- State A assigns City 1 in State A an OID of 1.3.6.1.4.1.65534.51.30.1, City 2 in State A an OID of 1.3.6.1.4.1.65534.51.30.2, etc., where .30.x is a city.
- State A then assigns Transportation Agency α in State A an OID of 1.3.6.1.4.1.65534.51.31.1, and Transportation Agency β and OID of 1.3.6.1.4.1.65534.51.31.2., etc., where .31.x is transportation agency.
- State A's reasoning is that sub arc .51 is assigned to State A, while the next level sub arc identifies the region or a type of organization (city, transportation agency), while the next sub arc identifies a specific organization.

Thus, if Region 1 in State A assigns an intersection with the identifier of 256, its OpOrgID is 1.3.6.1.4.1.65534.51, DE_RelativeRoadAuthorityID is 1, and DE_IntersectionID is 256.

If City 1 in State A assigns an intersection with the identifier of 5001, its OpOrgID is 1.3.6.1.4.1.65534.51, DE_RelativeRoadAuthorityID is 30.1, and DE_IntersectionID is 5001.

EXAMPLE:

Intersection 5001 in the example above broadcasts a SPaT and MAP message. The structure of the SPaT and MAP message is:

SPaT:

{"id":5001, -- DE_RoadRegulatorID is omitted

"revision":1, ….

"relRdAuthID":30.1} -- CHOICE of DE_RelativeRoadAuthorityID

MAP:

{"msgIssueRevision":1,"id":5001, -- DE_RoadRegulatorID is omitted

"revision":2,…

"relRdAuthID":30.1} -- CHOICE of DE_RelativeRoadAuthorityID

A.1.4 Implementation Issues

There are several potential implementation issues that have not been resolved at the time of the publication of this implementation guide.

- Different certificate holders or organizations within the same region may wish to coordinate to avoid assigning the same intersection identifier (DE_IntersectionID). Although the overall intersection identifier (with the OpOrgID, DE_RelativeRoadAuthorityID, and DE_IntersectionID) may be unique, the OpOrgID has to be extracted from the signing certificate, so it may be less confusing for receivers of messages if different intersection identifiers are used within a region (e.g., within the broadcast range of an RSU). The potential confusion exists regardless of if the certificate holder is the same organization or different organizations for both intersections.

- SCMS providers may choose to publish their OpOrgID assignments, but are not required to do so. If not, the identity of an OpOrgID may not be publicly known.

ANNEX B - USER REQUESTS [INFORMATIVE]

This annex identifies needs, requirements, and design details identified and considered by the CTI Committee or its task forces but are not included. The rationale on why these needs, requirements, and design details is not included is also provided. This section is included for consideration for future editions of CTI 4501.

B.1 USER REQUESTS - NEEDS

This section identifies user needs that are identified and considered by the CTI Committee or its task forces.

B.1.1 Mobility Applications

The CTI Committee primarily did not consider user needs for mobility applications for this version of CTI 4501. As stated in 5.4, only user needs to support the RLVW application are considered due to time and resource constraints. Needs to support SPaT-based and MAP-based safety and mobility applications are considered if the requirements to satisfy those needs and the design to fulfill those requirements can be completely defined within the project schedule.

B.1.2 Queue Information at an Intersection

The CTI 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.

B.1.3 Indication of Pedestrians or Bicyclists in a Crosswalk

The CTI 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.

B.1.4 Confidence Factor and Likely Time

The CTI 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% 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.

B.1.5 Signal Priority and Preemption

The CTI 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 RLVW implementation should neither preclude SRM and SSM nor SPaT messages and signal timing changes based on these messages." The CTI Committee decided that there were insufficient time and resources to address this need at this time.

B.1.6 Advisory Speeds

The CTI 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 with field testing to define requirements and testing approaches.

B.1.7 Misbehavior Reporting by OBUs

The CTI 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 CTI Committee agreed this need is out of scope at this time and could require a large amount of effort. The CTI 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.

B.1.8 Misbehavior Reporting by IOO Field Devices

The CTI 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 CTI Committee agreed this need is out of scope at this time and could require a large amount of effort. The CTI Committee also noted this need is not addressed by any group/standard right now.

B.1.9 Levels of Testing [Deprecated]

The CTI Committee considered a need, "The CI test methodology needs to define Levels of Testing." However, the CTI Committee agreed there was insufficient time to address this need at this time.

NOTE: This user request was deprecated in CTI 4501 v02 because the topic is addressed in Annex D.

B.2 USER REQUESTS - REQUIREMENTS

This section identifies requirements that are identified and considered by the CTI Committee or its task forces but are not addressed in CTI 4501.

B.2.1 Quality Assurance

The CTI Committee considered requirements on Quality Assurance. However, the SPaT/MAP Task Force decided that there were insufficient time and resources to specify 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 timestamp.

- 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.

B.2.2 Computed Lane - Scaling

The CTI Committee considered requirements for scaling (X-axis and Y-axis); however, there are 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 are unclear. The requirement 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. The scale factor is measured in 0.05 percent increments with positive values indicating that the computed lane is larger than the referenced lane."

B.2.3 No SPaT Available

The CTI 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 CTI 4501.

B.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 v03 was to address the deficiencies in v02. Currently, we recognize that there are even more clarifications necessary to ensure an interoperable environment and have taken the steps to recommend clarifications to the standards (among them NTCIP 1202) in CTI 4501. These clarifications in CTI 4501 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 v03 standard using clarifications in CTI 4501 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 CTI Committee does not recommend deploying TSCBM at new locations.

B.3 USER REQUESTS - DESIGN DETAILS

This section identifies design details that are identified and considered by the CTI Committee or its task forces but are not addressed in CTI 4501.

B.3.1 Failure Flash

The CTI 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 need to be defined in more detail, including guidance on how to be more complete in reporting all forms of failure flash.

B.3.2 Operational Logging - TSC Infrastructure

The CTI 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 are 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.

B.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.

B.3.4 Test Cases

The CTI 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 CTI Committee deferred developing test cases to fully validate and verify CTI 4501. However, the CTI Committee did develop Section 8, Connected Intersection Testing, 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.

B.3.5 Security Models

Consider which SNMP security models are permissible, in coordination with NTCIP and with any RSU standard updates.

ANNEX C - RECOMMENDATIONS TO STANDARDS DEVELOPMENT ORGANIZATIONS [INFORMATIVE]

This annex summarizes comments and recommendations by the CTI Committee or its task forces to SDOs on existing standards that are referenced by CTI 4501.

C.1 SAE CORE TECHNICAL COMMITTEE - SAE J2735

This section identifies comments and recommendations by the CTI Committee for SAE J2735, "V2X Communications Message Set Dictionary."

C.1.1 DE_TimeMark [Deprecated]

In CTI 4501 v01, the CI Committee recommended that the description of DE_TimeMark be improved in two ways. Refer to CTI 4501 v01 Annex H.1.1. for the exact text.

NOTE: This recommendation is deprecated in CTI 4501 v02 because text was added in SAE J2735_202211: "If the value of TimeMark is greater than the current time, it applies in the current hour, and if it is less than the current time, it applies in the next hour." In addition, the note for TimeMark was updated to, "-- In units of 1/10th second from UTC time in the current or next hour."

C.1.2 DF_MovementEventList [Deprecated]

In CTI 4501 v01, the CI Committee requested a minor change in the language describing DE_MovementPhaseState. Refer to CTI 4501 v01 Annex H.1.2 for the exact text.

NOTE: This recommendation is deprecated in CTI 4501 v02 because the text was updated in SAE J2735_202211 to: "The DE_MovementPhaseState data element provides the overall state of the movement…."

C.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 backward compatibility, no change is needed unless the bits are needed.

C.1.4 DF_NodeAttributeSetLL [Deprecated]

In CTI 4501 v01, the CI Committee noted that there may have been a typo in the description for dElevation. Refer to CTI 4501 v01 Annex H.1.4 for the exact text.

NOTE: This recommendation is deprecated in CTI 4501 v02 because the text was updated in SAE J2735_202211 to, "in 1 cm steps."

C.1.5 DE_RoadRegulatorID [Deprecated]

In CTI 4501 v01, the CI Committee expressed their concerns with implementing DE_RoadRegulatorID. Refer to CTI 4501 v01 Annex H.1.5 for the exact text.

NOTE: This recommendation is deprecated in CTI 4501 v02 because DE_RelativeRoadAuthorityID was added in SAE J2735_202211 as a more extensible means of identifying IOOs.

C.1.6 DF_TimeChangeDetails [Deprecated]

In CTI 4501 v01, the CI Committee requested clarification on the use of startTime. Refer to CTI 4501 v01 Annex H.1.6 for the exact text.

NOTE: This recommendation is deprecated in CTI 4501 v02 because the note for startTime was updated in SAE J2735_202211 to: "-- when this future phase will start."

C.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 CTI 4501. Examples of requirements that may result in large MAP message sizes include the following:

- CTI 4501/2 sections 6.3.3.4.1.7 to 6.3.3.4.1.9, which require that all permitted vehicle lanes, crosswalk lanes, and pedestrian landings be identified.
- CTI 4501/2, 6.3.3.4.1.17, Advanced Notification - Ingress Vehicle Lane, which requires that each ingress vehicle lane extend a minimum distance from the first node point of the lane.
- CTI 4501/2, 6.3.3.4.1.20, 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.

C.1.8 Backward Compatibility

The CI Committee respectfully asks SAE not to make changes to a SAE J2735_202007 data element that would break backward 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.

C.1.9 DE_IntersectionStatusObject

The Committee respectfully asks SAE to define Bit 14 as follows:

noValidRTCMisAvailableAtThisTime (14)

-- RTCMcorrections Message is not available or is invalid at this time

This change allows the CTI Committee to add a requirement as follows:

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

If a connected intersection does not have a valid RTCMcorrections message to broadcast

With the design:

Whether an RSU is broadcasting a valid RTCMcorrections message is represented by Bit 14 in the DE_IntersectionStatusObject and found under the data frame DF_IntersectionState in MSG_SignalPhaseAndTiming Message in SAE J2735.

A value of 0 for Bit 14 indicates that the RSU is broadcasting a properly formatted RTCMcorrections message. A value of 1 for Bit 14 indicates that either the RTCMcorrections is unavailable, or it is invalid.

NOTE: This recommendation was added in CTI 4501 v02.

C.2 NTCIP ACTUATED SIGNAL CONTROLLERS (ASC) WORKING GROUP

This section identifies comments and recommendations by the CI Committee for NTCIP 1202 v03A.

C.2.1 Protected/Permissive Movements [Deprecated]

In CTI 4501 v01, the CI Committee requested clarification on how to differentiate between protected and permissive movements as stated in NTCIP 1202 v03A. Refer to CTI 4501 v01 Annex H.2.1 for the exact text.

NOTE: This recommendation was deprecated in CTI 4501 v02 because the design was updated in NTCIP 1202 v03b to allow the IOO to unambiguously indicate if a movement is permissive or protected.

C.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. Refer to A.2.1.6, Hard Flashing Operation, in CTI 4501 v01. Flash color is often hardwired in the traffic cabinet using jumpers or plugs such that the controller is unaware of what colors are flashing.

C.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. Refer to A.2.1.10, Output Mapping, in CTI 4501 v01.

C.2.4 Output Mapping [Deprecated]

The CI Committee recommended 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. Refer to A.2.1.10, Output Mapping, in CTI 4501 v01. Refer to CTI 4501 v01 Annex H.2.4 for the exact text.

NOTE: This recommendation was deprecated in CTI 4501 v02 because the design was updated in NTCIP 1202 v03b to support lookup tables to map phase and overlap outputs relative to the signal group ID and movement states.

C.2.5 Additional SPaT Elements [Deprecated]

The CI Committee recommended that object definitions be created to support additional data elements required to generate a SAE J2735_202007 SPaT message. Refer to CTI 4501 v01 Annex H.2.5 for the exact text.

NOTE: This recommendation was deprecated in CTI 4501 v02 because the design was updated in NTCIP 1202 v03b to support startTime and DE_RelativeRoadAuthorityID.

C.2.6 SPaT Data Tables [Deprecated]

In CTI 4501 v01, the CI Committee asked 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. Refer to CTI 4501 v01 Annex H.2.6 for the exact text.

NOTE: This recommendation was deprecated in CTI 4501 v02 because the design was updated in NTCIP 1202 v03b to support multiple interval states.

C.3 NEMA TS2 WORKING GROUP

There is a risk a DC isolator failure may remove controller awareness of flashing conditions. The 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. Refer to A.2.1.6, Hard Flashing Operation, in CTI 4501 v01.

C.4 ATC JOINT COMMITTEE/ITS CABINET WORKING GROUP

There is a risk a DC isolator failure may remove controller awareness of flashing conditions. The 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. Refer to A.2.1.6, Hard Flashing Operation, in CTI 4501 v01.

C.5 CTI 4001

This section identifies comments and recommendations by the CTIC for CTI 4001.

C.5.1 SubjectAltName

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. The client certificate is contained within the certificate "allow list"; however, the "allow-list" does not accommodate the frequently changing nature of client certificates. A design using SubjectAltName and naming pattern is preferred, so the CTIC requests that CTI 4001 be updated to use the SubjectAltName field in the client certificate such that it matches an IOO-specific naming pattern (e.g., to distinguish between certificates from the same root certificate authority but for different IOOs).

NOTE: This recommendation is added in CTI 4501 v02.

ANNEX D - RLVW DEPLOYMENT - PRACTITIONER APPROACH [INFORMATIVE]

D.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 addresses the following topics:

- What expectations are for the CI with deployed RLVW applications and how these goals can be satisfied.
- How to deploy a CI on a new intersection or upgrade existing intersections to support the RLVW application.
- What important resources, approaches, and best practices which an agency can follow to deploy and maintain a CI over the long term.

The main audience for this section includes transportation agencies, IOOs, infrastructure designers, system integrators, 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, this section assumes that the reader has a basic understanding of the CV technology, its basic approaches and building blocks, and some experience in planning and deploying of the CV infrastructure. Section C.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.

D.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.

D.1.1.1 Delivers Expected Performance and Accuracy

The CI is expected to support a wide range of safety applications, including RLVW and 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 needs 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 ongoing 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.

D.1.1.2 RLVW Is Interoperable

It is anticipated that CIs constructed in compliance with CTI 4501 will attain a significant level of interoperability with RLVW applications. 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 North America including Hawaii, Guam, and 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 remain available to the majority of system users.

D.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. Section 5.4.4 addresses security needs; and CTI 4501/3 addresses requirements and design approaches specific to the CI system. As an integral part of an operating agency's infrastructure, the CTI 4501 security requirements must be aligned and coordinated with the security approaches employed by the system operator for all of their other deployed systems.

D.1.1.4 Sustainable and Reliable

The connected intersection 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 connected intersection.

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 are challenges that 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 correct 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 the connected intersection extremely reliable.

D.2 ARCHITECTURAL VIEWS

The purpose of this section is to use architecture diagrams to showcase systems, services, and functions required to deploy and operate the CTI. It also highlights 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.

This section acknowledges 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 CTI 4501 requirements.

D.2.1 Services View

The Services View architecture is shown in Figure D1. It includes architecture elements which are expected when the CI system is fully implemented with the capabilities known at the time of publication.

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 does include OBU representation to highlight that OBUs are critical to the integration and some OBUs managed by IOOs (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.

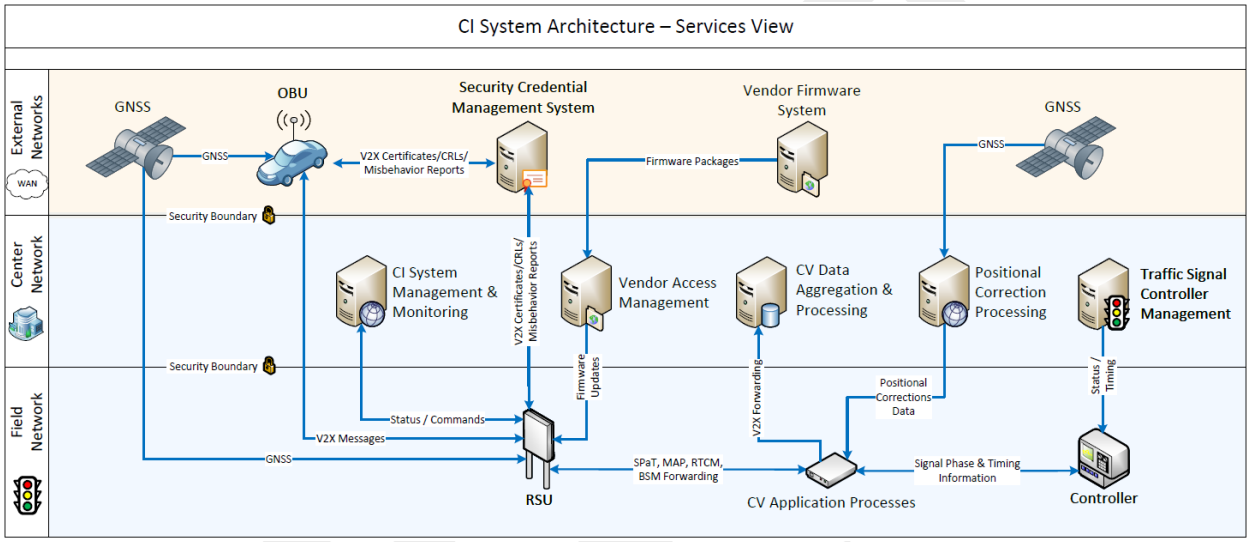


Figure D1 - CI system architecture - Services view

Table D1 discusses main functionality and services provided by the various elements presented in Figure D1.

Table D1 - Services and functionality represented in Figure D1

Component	Provided Services/Functionality
Field Network	Encompasses systems and services deployed in the field.
Controller (Traffic Signal Controller or TSC)	• 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 in Figure D1.
CV Application Processes	• Supplemental processing required to facilitate data exchanges between TSC and RSU, and Positional Reference System and RSU. • Receives and 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, etc. • Maintenance of RSU configuration/databases ***Additional notes:*** • CV Application Processes may be implemented in the External Control Local Application (ECLA) processor. • The combination of TSC and ECLA is referred to 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)	• Transmission/reception of V2X messages (i.e., SPaT, MAP, BSM, RTCMcorrections) 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 RTCMcorrections. • 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 back-office network
Traffic Signal Controller Management	• 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	• 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.
CI System Management and Monitoring	• Agency control over CI system. RLVW application performance monitoring. Exception detection due to hardware/software failures. System configuration management, backup, and restore.
Firmware Management	• Agency control over software provisioning and updates for RSUs, ECLAs, and other roadside components.

Component	Provided Services/Functionality
CV Data Aggregation and Processing	• 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	• 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	• 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	• 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	• 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)	• 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	• 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 subdomains.

Table D2 - Interconnections in Figure D1

Flow label	1st end	2nd end	Description, Examples of data
Signal Phase & Timing Information	Controller (Traffic Signal Controller)	CV Application Processes	• Signal status and timing information generated by the Controller is used to create SPaT messages.
SPaT, MAP, RTCM, BSM Forwarding	CV Application Processes	RSU	• SPaT, MAP, and RTCMcorrections messages if CV Application Processes are used to create them. Otherwise, this flow passes through to the RSU where the messages are generated and transmitted by the RSU • Information is extracted from processed BSMs and sent to the Controller for the AGP application.
Signal/Timing	Traffic Signal Controller Management	Controller	• Controller timing plans, controller databases, settings, events.
GNSS	GNSS	Position Correction Processing	• Positional correction information collected from CORS before it is processed into RTCM.
Positional Corrections data	Position Correction Processing	CV Application Processes	• Positional correction information filtered and tailored to the CI deployment footprint.
V2X Forwarding	CV Data Aggregation & Processing	CV Application Processes	• 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	• 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	• Approved software updates, patches to be applied to RSUs and other field devices.

Flow label	1st end	2nd end	Description, Examples of data
V2X Certificates/ CRLs, Misbehavior Reports	Security Credential Management System	RSU, OBU	• 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	• Status information and control commands use to monitor and manage the CI system.
V2X Messages	OBU	RSU	• V2X messages, e.g., SPaT, MAP, RTCMcorrections and BSMs exchanged between RSU and OBU.

The Services View provides a "typical" view of the architecture system. This view is intended as a guidance to help an agency to define their own implementation. Though the diagram resembles a 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 architectures 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 Network Transport of RTCM via Internet Protocol (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 an IOO's ability to sustain operations through multiple iterations of software and configuration changes. Therefore, having these elements included in 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 networks.

D.2.2 Communications Architecture

The Communications View is shown in Figure D2. It depicts three layers common with the Services View (see Figure D1). It also refers to several elements using the same names as in Figure D2. Its emphasis is to show different communication options for data exchanges between Field Network devices, Center Network systems, and External Network systems.

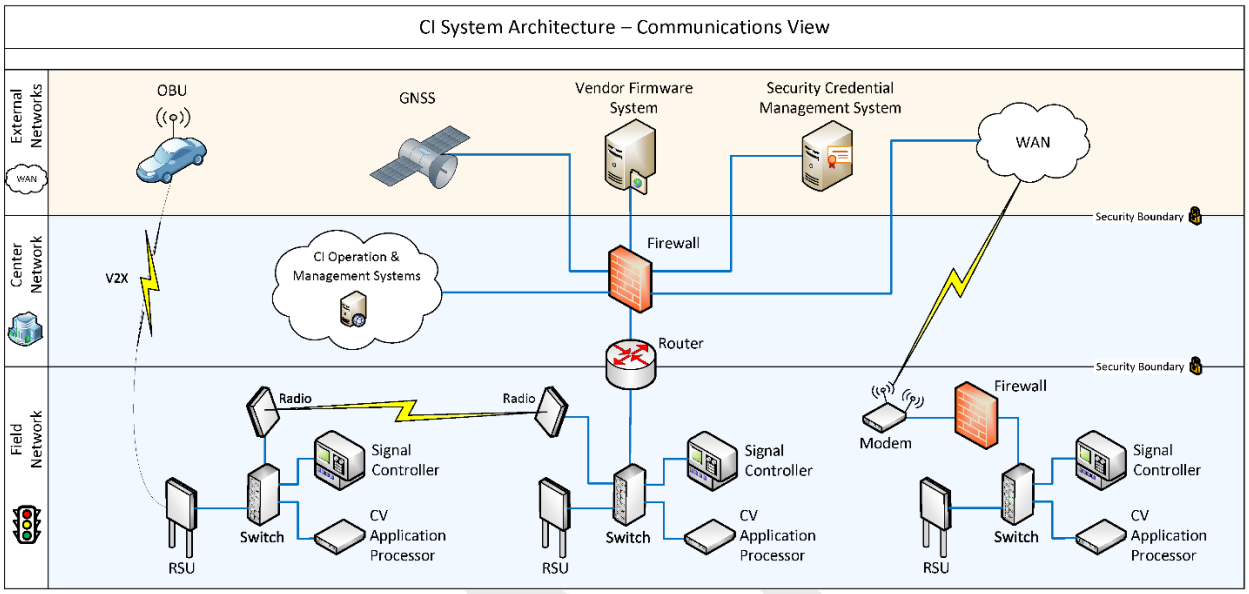


Figure D2 - CI system architecture - Communications view

A deploying infrastructure owner may operate an existing hybrid network consisting of multiple mediums and pathways for communication from the field to their Center Network. To illustrate how an agency might leverage these different mediums in deployment, the Communications View diagram in Figure D2 depicts three representative (but not exhaustive) network architecture options connecting CI systems in the field to supporting systems in the Center Network and/or External Networks. Each depicted intersection includes a representative collection of devices typical for a CI system (a TSC, RSU, CV Application Processor, and network communications devices):

- On the left, a CI system lacks available fiber optic or other hardline network mediums, but is nearby to an intersection that features those connections, so a point-to-point wireless link is installed between them to facilitate the CI's connection to the Center Network.

- In the middle, the CI system with a hardline connection has a direct network path back to the Center Network, passing through a Router and the Center Network security boundary before reaching the resources there.

- On the right, a CI exists without proximity to existing network infrastructure, so the agency has deployed a cellular internet modem for connectivity. Since there is not a direct path into the Center Network, and the CI must connect through the internet, a field security appliance (firewall) is installed behind the modem to protect the CI devices and provide secure communications.

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:

- The CI system requires RSUs to operate with security certificates. For RSUs to access SCMS certificates provided by the Security Credential Management System, network path and security rules are put in place within the Field and Center layers.

- A similar consideration is required if an External Positional Reference System is utilized. Network and security rules must be established to allow position correction messages to reach RSUs.

- As highlighted by network examples in the Field Network segment in Figure D2, a number of options are available to connect to the field devices ranging from fiber, wireless, cellular, and other options as long as they can fulfill system requirements for network security and bandwidth for CI system monitoring.

- Robust and secure communication between field devices and center network systems is essential to collect CV data from vehicles for processing and system monitoring. Certainly, data processing at the edge can significantly reduce the need for bandwidth; however, a robust network is still important for system monitoring and to facilitate data collection and archiving for post-processing.

- Any network will work as long as it is secure (segmented), reliable, and can handle large volumes of data if BSMs are forwarded for the CV Aggregation and Processing.

- A good understanding of an agency's network is important for V2X deployment.

- A hybrid network with a variety of mediums may necessarily create network pathways with security boundaries an agency may not normally anticipate. For example, the CI system on the far right of the diagram using a cellular modem is connecting to an External Network (the internet) before reaching the agency's Center Network. In this case, the agency must of course protect the field devices themselves, but will also need to facilitate connections through an External Network boundary that are normally assumed to come through a more trusted Field Network boundary. Some agency IT departments may have security policies against such communications paths that would warrant special exceptions or a re-architecting of the agency's planned deployment.

During earlier CV pilot deployments, SPaT/MAP deployments were done with low bandwidth data and sometimes without connection to an SCMS. This Communication View diagram highlights that a fully implemented CI system will require connection to an SCMS and expect real-time system monitoring to be performed. Monitoring will be particularly important, as the system increases in the number of deployed nodes and system operational monitoring and security involves a larger number of intersections.

D.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, it is anticipated 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 RLVW applications described in CTI 4501.

Hundreds 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 ECLAs. Upgrading these sites could offer a straightforward path to implement RLVW requirements outlined in CTI 4501.

Table D3 summarizes the scope of implementation required for the CI. These changes are requirements to be considered a connected intersection, even for intersections that already broadcasts SPaT and MAP messages. The list below assumes that any configuration changes are implemented as part of the corresponding component implementations.

Table D3 - Upgrade path from existing SPaT/MAP broadcast sites to the CI system

	Component	Expected changes
	Field Network	
1.	Install RSUs	• 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 traffic cabinet	• 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 TSCs can be updated using a software update. Some intersections may require 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	• 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 back-office	• Network link between traffic cabinets and back-office 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. This requirement may be fulfilled by several design approaches as depicted in Figure D2.
5.	Support broadcast of SPaT, MAP, and RTCMcorrections messages	• RSU must support the interface with the TSC and be capable of broadcasting SPaT and MAP messages as specified in CTI 4501. • RSU must support broadcasting RTCM messages as per SAE 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 to sign them and transmit over-the-air.
6.	MAP changes	• MAP messages may need reevaluation and validation per SAE J3238/2. GIS surveyor grade equipment may be required to achieve the required precision of GIS data used to create MAP messages. • MAP messages require periodic updates to reflect intersection changes due to road construction, lane changes, consistency with SPaT, etc.
7.	System validation	• 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 4501/3, 7.3.4.1.1. • 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	• Every operational CI system is expected to be registered with 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	
9.	CI monitoring system	• Deploying a 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	• All components of the CI require periodic software upgrade. Ensure that secure provisioning of software updates is available for all CI components.

D.4 IMPORTANT CONSIDERATIONS FOR CI DEPLOYERS AND OPERATORS

This section provides a summary of best practices derived from lessons learned from the deployment of a 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 requires 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 connection 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 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, 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 and Security: The CI system is expected to have access to services that may reside in different network domains or even outside of an IOO network, e.g., SCMS, cloud data storage, CORS network, system monitoring, and 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: Accurate time synchronization is required between RSUs and TSCs. Time synchronization is important because signal phase and timing information generated by TSCs are interpreted and translated into SPaT messages which is often performed by RSUs. By virtue of having an integrated positioning system (e.g., 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 Network Time Protocol (NTP) or Precision Time Protocols (PTP) 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 RTCMcorrections messages and verify signatures of incoming BSM messages. RSU signing certificates will typically last for 1 to 2 weeks. Therefore, each RSU will be periodically reaching out to an SCMS provider and downloading new certificates and CRLs. Ensuring that all RSUs have up-to-date certificates can be an important service provided by the CPMS.

- Ongoing 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 a 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 that the functions of ECLAs may be absorbed into other devices and the need to deploy ECLAs will diminish.

- 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 sooner and saving on field troubleshooting.

- OBU Life Cycle: Even though some IOOs will deploy their own OBUs in their fleet vehicles, it is expected 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 life cycle 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 life cycles, 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 ongoing 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.

D.4.1 Anticipated Changes in RLVW Environment

As technology continues to evolve, those responsible for implementing RLVW 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 D.5.1 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/releases 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 ongoing 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 dates 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, and TMCs. 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 geometries described in MAP files and actual vehicle trajectories and alert operators for an action (e.g., temporarily disable RLVW application until discrepancy is resolved).

D.5 USEFUL REFERENCES AND OTHER RESOURCES

D.5.1 Key Standards for System Deployment and Interoperability

There are several industry standards that provide backbone requirements to ensure system interoperability for CTI. As CV technology continues to evolve, the standards are expected to change and periodically be revised. It is recommended to monitor the following standards for version updates and update device procurement documents to ensure interoperability and support technological evolution. Table D4 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. Table D5 lists other references that should be consulted for deployment and interoperability.

To avoid duplications, Tables D4 and D5 omit listing specific versions of standards and refers the reader to consult Section 2.

Table D4 - Backbone standards

Identifier + Title	Summary	Impact
CTI 4501 Connected Intersections Implementation Guide	This document	Any changes to this document 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 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 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 and MIBs with an Actuated Signal Controller Unit and establishes an interface between the TSC and a CV Roadside process such as an RSU.	Changes to 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.

Table D5 - Other references

Identifier + Title	Summary
Connected Intersection Guidance Document	Summary of best practices for the deployment of a connected intersection.
CVPFS Guidance Document for MAP Message Preparation	Discusses best practices for creating MAP messages.
ISD Message Creator	USDOT tool for creating MAP messages using satellite maps
V2I Hub Deployment Guide	Checklist for a successful deployment of the V2I Hub platform that facilitates communication between connected vehicle hardware and traffic control systems.
V2X Hub Software Repository	USDOT software repository for the V2X Hub.

D.6 CONSIDERATIONS FOR CI ONGOING OPERATIONS AND MAINTENANCE

This section discusses approaches for CI operations and maintenance in order to meet the system operating goals.

D.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 ongoing 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.
- Integrate CTI security with the agency-wide cyber security organizational practices.
- Consider participating in various industry forums (e.g., CTI Committee, CVPFS) to share and learn about industry best practices, validation, and interoperability initiatives.

ANNEX E - REVISIONS FROM CTI 4501 V01 [INFORMATIVE]

This section identifies the changes that have been made to CTI 4501. The Technical Committee makes reasonable efforts to ensure that documents are as backward compatible as possible, but the primary purpose of these documents is to provide interoperability by developing implementation guides in a consensus environment. When changes are required to meet these objectives, the problematic elements, such as user needs, requirements, and design guidance, are refined (if the issue is primarily editorial) or deprecated and, in most cases, replaced with updated needs, requirements, and guidance. This annex identifies why each of these changes has been made.

E.1 CHANGES TO USER NEEDS

The following identify changes from CTI 4501 v01 to CTI 4501 v02 for user needs.

E.1.1 Security User Needs

The user needs for security (Section 5.4.4.x) are NOT backward compatible with the security user needs in CTI 4501 v01.

E.2 UPDATES TO REQUIREMENTS

The following identify changes from CTI 4501 v01 to CTI 4501 v02 for requirements.

E.2.1 Deprecated DSRC

Removed 3.3.1.1, IEEE Std 802.11-2016 (DSRC), and all child requirements in CTI 4501 v02 because the United States Federal Communications Commission (FCC)'s Second Report and Order on the *Use of the 5.850-5.925 GHz Band* vacates the use of DSRC communications technology in the 5.9 GHz band after several years.

E.2.2 Deprecated One Short Transmission

Deprecated 3.3.1.2.2, One Shot Transmission, in CTI 4501 v02 because the recommendations for when one shot transmissions are in SAE J3161 and earlier requirements already point to SAE J3161.

E.2.3 Updated NRTM - Time Accuracy

Updated the NRTM so 3.3.3.2.1, Time Accuracy, only applies to SPaT and RTCMcorrections messages. This requirement does not apply to MAP messages.

E.2.4 Deprecated SPaT Information Message Performance Requirements

Deprecated 3.3.2.1.2, TSC Infrastructure SPaT Information Message Transmission Rate; 3.3.2.1.3, TSC Infrastructure SPaT Information Message Transmission Failure Threshold; 3.3.2.1.4, TSC Infrastructure SPaT Information Average Message Update Latency; and 3.3.2.1.5 TSC Infrastructure Processing Latency in CTI 4501 v01 and replaced these four requirements with 6.3.2.1.6, TSC Signal State Periodicity, and 6.3.2.1.7, TSC Signal Indication Phase State and SPaT Information Consistency.

E.2.5 Deprecated SPaT Message Performance Requirements

Deprecated 3.3.3.1.5.1, SPaT Message - Broadcast Periodicity, and 3.3.3.1.5.2, SPaT Message - Broadcast Latency in CTI 4501 v02, and replaced these two requirements with 6.3.3.1.5.1, SPaT Message - Broadcast Latency and Accuracy - Commanded.

E.2.6 Deprecated RTCMcorrections Message - Sequence Number Not Increment

Deprecated 3.3.3.2.2.8, RTCMcorrections Message - Sequence Number Not Increment, in CTI 4501 v02 because the requirement is determined to be unnecessary.

E.2.7 Deprecated Road Regulator Requirements

Deprecated 3.3.3.3.1.2, Road Regulator Identifier, and 3.3.3.4.8.1, Matching Intersection Reference Identifier from CTI 4501 v01.

See Section A.1 for a detailed explanation and guidance.

E.2.8 Deprecated Walk State Enumeration (Potential Conflict)

Deprecated 3.3.3.3.3.9, Walk State Enumeration (Potential Conflict), from CTI 4501 v01. This requirement was deprecated in CTI 4501 v02 because the definition of a protected movement was updated. All pedestrian movements with a WALK indication have the right of way. Using permissive-Movement-Allowed would tell the pedestrian they must yield to conflicting traffic even though they have the WALK indication, which is not the case.

E.2.9 Deprecated Intersection Reference Point Accuracy

Deprecated 3.3.3.4.1.4.3, Intersection Reference Point Accuracy, from CTI 4501 v01. This requirement was deprecated in CTI 4501 v02 because the accuracy requirement is already embedded into the requirement for the first node point position of each lane. Refer to CTI 4501/2, 6.3.3.4.1.11 and 6.3.3.4.1.12.

E.2.10 Deprecated Node Accuracy

Deprecated 3.3.3.4.1.23, Node Accuracy, from CTI 4501 v01. This requirement was deprecated in CTI 4501 v02 because the accuracy requirement is already embedded into the requirement for the first node point position of each lane. Refer to CTI 4501/2, 6.3.3.4.1.11 and 6.3.3.4.1.12.

E.2.11 Moved Topic-Specific Requirements and Design Details

Moved SPaT-specific requirements and design details to CTI 4501/1 including 3.3.2, TSC Infrastructure to RSU Requirements; 3.3.3.3, Signal Timing Data Requirements; 4.3.2, TSC Infrastructure to RSU Design Details; and 4.3.3.3, Roadway Geometry Data Design Details; from CTI 4501 v01.

Moved MAP-specific requirements and design details to CTI 4501/2 including 3.3.3.4, Road Geometry Data Requirements, and 4.3.3.4, Roadway Geometry Data Design Details, from CTI 4501 v01.

Moved Positioning (RTCM)-specific requirements and design details to SAE J3258 including 3.3.3.5, Positioning Messages, and 4.3.3.5, Positioning Messages, from CTI 4501 v01.

Moved Security-specific requirements and design details to CTI 4501/3 including 3.3.4, Security Requirements, and 4.3.4, Security Design Details, from CTI 4501 v01.