SURFACE VEHICLE RECOMMENDED PRACTICE	CTI 4501™/4	PropDft FEB2026
	Issued	Proposed Draft 2026-02-02

Connected Intersections Implementation Guide - Testing and Validation Guidance

RATIONALE

The Connected Intersection (CI) Implementation Guide (CTI 4501) was 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 was supported by the United States Department of Transportation (USDOT) Intelligent Transportation Systems (ITS) Joint Program Office (JPO). Several associations, such as the American Association of State Highway Transportation Officials (AASHTO), the Institute of Transportation Engineers (ITE), the National Electrical Manufacturers Association (NEMA), and SAE International, contributed to ensuring balanced and effective stakeholder representation and adherence to standards development processes as Standards Development Organizations (SDOs).

The CTI 4501 family of documents are recommended practices 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, the 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, especially for automated transportation systems. Building on the USDOT-sponsored Cooperative Automated Transportation Clarifications for Consistent Implementations (CCIs) for Connected Signalized Intersections, the CI Implementation Guide focuses on harmonizing the messages broadcasted by connected intersections.

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.

The CTI 4501 family of documents define 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, these recommended practices provide 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 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 CTI 4501, 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), System Requirements (Functional Requirements), System Design Details, and a Needs to Requirements Traceability Matrix (NRTM). 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. By separating out these focused topics, the guide more effectively supports Infrastructure Owner Operators (IOOs), OEMs, suppliers, and application developers who need targeted information. Taken together, the main 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.

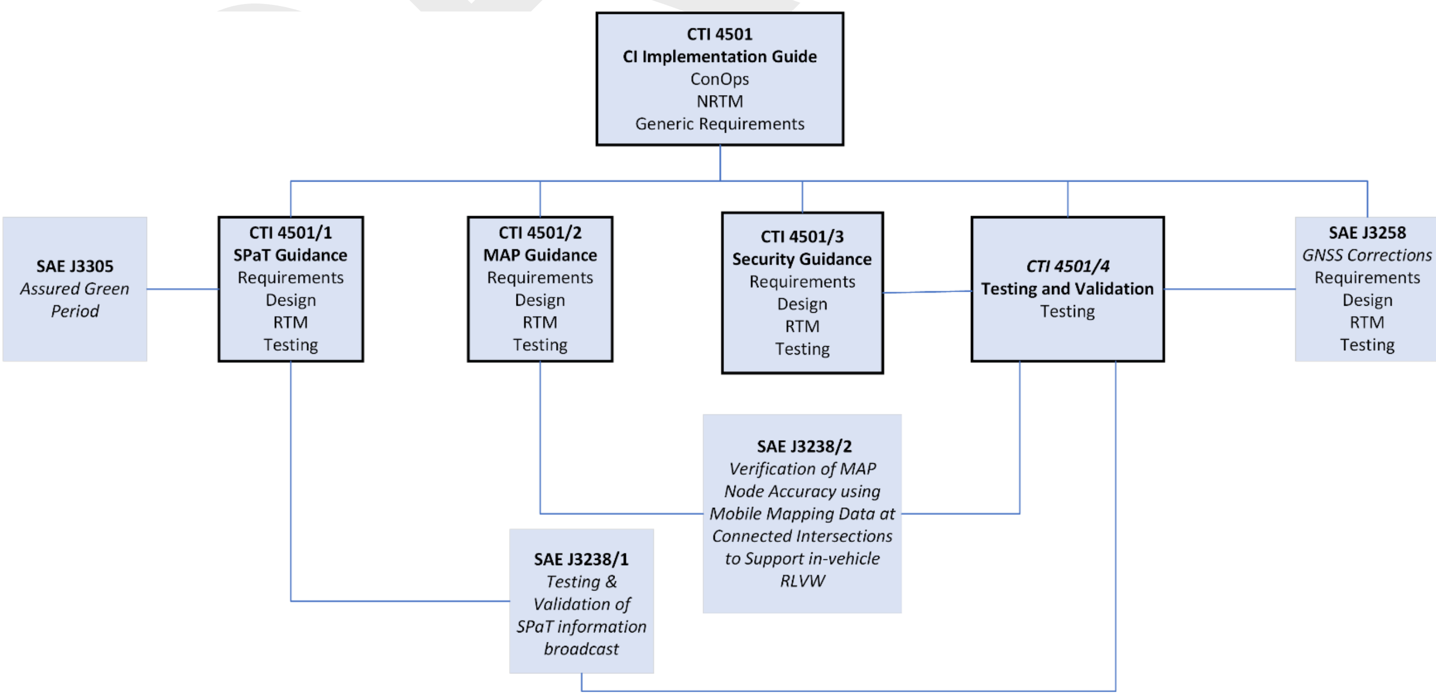

Figure 1 - Relationship with other documents

This Testing and Validation Guidance Document focuses on providing guidance on developing a verification plan to confirm that an implementation fulfills all the requirements for a connected signalized intersection. This document defines what should be included in, and examples of content that should go into a verification plan.

For IOOs, this document provides actionable guidance on developing test documents to verify an implementation for interoperability. The contents of this document are NOT standardized test methods, test cases, or test procedures; instead, the contents are EXAMPLES of what might be in a verification plan. The specific test approach, test scope, test cases, and test procedures in a verification plan will vary by IOO based on its specific test approach, procedures, and policies.

For OEMs and developers, how an IOO will verify an implementation such that the connected vehicle messages broadcasted from compliant intersections enables the development of standards-based safety-critical applications such as Red Light Violation Warning (RLVW). Users are encouraged to refer to the main CTI 4501 document for overarching ConOps, system needs, and operational context while leveraging this Testing and Validation guide for verification and validation activities.

Other companion documents, such as CTI 4501/1 - SPaT Messages and CTI 4501/2 - MAP Messages, also contain content about connected intersection testing in Section 8. However, CTI 4501/4 provides the overview and philosophy of developing a testing framework in Section 8, while the companion documents provide topic specific examples.

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 J3161/1A	Vehicle Level Validation Test Procedures for V2V Safety Communications
SAE J3238/1	Testing and Validation of Broadcast SPaT from V2X Connected Intersections (CI) Supporting In-Vehicle Red Light Violation Warning (RLVW) Application
SAE J3238/2	Verification of MAP Node Accuracy Using Mobile Mapping Data at Connected Intersections to Support In-Vehicle Red Light Violation Warning
SAE J3258	V2X Infrastructure Support for GNSS Corrections

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/rsu-standardization.

CTI 4001	Roadside Unit (RSU) Standard
CTI 4501	Connected Intersections (CI) Implementation Guide
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

2.1.3 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 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 1609.2.2	IEEE Draft Guide for Wireless Access in Vehicular Environments (WAVE) - Multi-Jurisdictional Interoperability Using Security Credentials Originating in Disparate Policy Domains

2.1.4 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)

2.1.5 SCMS Manager Publications

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

SCMS Manager Intersection Validation Policy

SCMS Manager – CI Test Results Report Format (developed as part of the Utah SMART Grant 2024)

2.1.6 U.S. Department of Transportation Publications

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

Connected Vehicle Pilots Phase 2 Interoperability Test: Test Report Final Report - November 9, 2018. Available from https://rosap.ntl.bts.gov/view/dot/39009/dot_39009_DS1.pdf.

Connected Vehicle Pilots Phase 2 Interoperability Test: Test Plan Final Report - August 13, 2018. Available from https://rosap.ntl.bts.gov/view/dot/36715.

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 J3287 V2X Misbehavior Reporting

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

2.2.2 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/rsu-standardization.

CTI 4502 Connected Intersections Validation Report: Findings from the Connected Intersections (CI) Project Validation Phase. Available at https://www.ite.org/technical-resources/standards/connected-intersections/.

2.2.3 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 802.3 IEEE Standard for Ethernet

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

2.2.4 ISO Publications

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

ISO/IEC/IEEE 15288 Systems and Software Engineering – System Life Cycle Processes

2.2.5 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

2.2.6 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

2.2.7 NTCIP Publications

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

NTCIP 1201	Global Object (GO) Definitions
NTCIP 2103	Point-to-Point Protocol over RS-232 Subnetwork Profile
NTCIP 2202	Internet (TCP/IP and UDP/IP) Transport Profile
NTCIP 2301	Simple Transportation Management Framework (STMF) Application Profile (AP) (AP-STMF)
NTCIP 9001	The NTCIP Guide

2.2.8 ATC Standards

ATC Standards are jointly developed by American Association of State Highway and Transportation Officials, Institute of Transportation Engineers, and National Electrical Manufacturers Association. Available at www.ite.org/technical-resources/standards.

ATC 5201	Advanced Transportation Controller Standard
ATC 5301	Advanced Transportation Controller Cabinet Standard (ATCC)

2.2.9 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.

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

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

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

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

2.2.11 Other Publications

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

3. DEFINITIONS

For the purposes of this recommended practice, 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 recommended practice, 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

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.

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) information, mapping information, and position correction data to On-Board Units (OBUs) and Mobile Units (MUs).

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

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

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

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.

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

SIGNAL GROUP ID: Data element in a SPaT message that represents traffic signal heads that control each possible movement of vehicles or travelers (e.g., pedestrians) at an intersection. See MOVEMENT.

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

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 this standard 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

4. ABBREVIATIONS

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

3GPP	3rd Generation Partnership Product
AASHTO	American Association of State Highway and Transportation Officials
AGP	Assured Green Period
ARC-IT	Architecture Reference for Cooperative and Intelligent Transportation
ASC	Actuated Signal Controller
ASN.1	Abstract Syntax Notation 1
ATC	Advanced Transportation Controller
AVD	Aftermarket V2X Device
BCD	Binary Coded Decimal
BSM	Basic Safety Message

CAMP	Crash Avoidance Metrics Partners
CAT	Cooperative Automated Transportation Coalition
CCI	Clarifications for Consistent Implementations (document)
CI	Connected Intersection
CMU	Conflict Monitor Unit
ConOps	Concept of Operations
CPMS	Connected Intersection Performance Monitoring System
CRL	Certificate Revocation List
CSV	Comma Separated Values
CTI	Connected Transportation Interoperability
CV	Connected Vehicle
DAT	Data Acquisition Tool
DTLS	Datagram Transport Layer Security
E2E	End to End
ECLA	External Control Local Application
EMI	Electromagnetic Interference
ESD	Electrostatic Discharge
E-UTRA	Evolved Universal Terrestrial Radio Access
FCC	Federal Communications Commission
FHWA	Federal Highway Administration
FTP	File Transfer Protocol
GNSS	Global Navigation Satellite System
I2V	Infrastructure-to-Vehicle
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INCOSE	International Council on Systems Engineering
IOO	Infrastructure Owner/Operator
ISO	International Organization for Standardization

ITE	Institute of Transportation Engineers
ITS	Intelligent Transportation Systems
IUT	Instrument Under Test
JPO	Joint Program Office
JSON	JavaScript Object Notation
LTE-V2X	Long-Term Evolution Vehicle-to-Everything
MIB	Management Information Base
MS	Microsoft
MU	Mobile Units
MUTCD	Manual of Uniform Traffic Control Devices
NEMA	National Electrical Manufacturers Association
NRTM	Needs to Requirements Traceability Matrix
NTCIP	National Transportation Communications for Intelligent Transportation Systems Protocol
NTRIP	Network Transport of RTCM via Internet Protocol
OBU	On-Board Units
OEM	Original Equipment Manufacturers
PoE	Power Over Ethernet
RLC	Radio Link Control
RLVW	Red Light Violation Warning
RSU	Roadside Unit
RTCM	Radio Technical Commission for Maritime Services
RTCTM	Requirements to Test Case Traceability Matrix
RTK	Real-Time Kinematic
SAE	SAE International
SCMS	Security Credential Management System
SD	Security Documents
SDLC	Synchronous Data Link Control
SDO	Standards Development Organization
SEP	Systems Engineering Process

SIU	Serial Interface Unit
SMART	Strengthening Mobility and Revolutionizing Transportation
SPaT	Signal Phase and Timing
TLS	Transport Layer Security
TMS	Traffic Management System
TSC	Traffic Signal Controller
TSCBM	Traffic Signal Controller Broadcast Message
TSP	Transit Signal Priority
UPER	Unaligned Packed Encoding Rules
USDOT	United States Department of Transportation
UTC	Coordinated Universal Time
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
WAVE	Wireless Access in Vehicular Environments
WIP	Work in Progress

5. CONCEPT OF OPERATIONS

Refer to CTI 4501 Section 5, Concept of Operations, for the user needs and operational scenarios.

6. FUNCTIONAL REQUIREMENTS

The functional requirements are defined in different CTI 4501/x documents based on the topic.

Refer to CTI 4501 Section 6, Functional Requirements, for general functional requirements that apply to the connected intersection and all messages based on the user needs identified in the Concept of Operations; and the Needs to Requirements Traceability Matrix.

Refer to CTI 4501/1 Section 6, Functional Requirements, for functional requirements for SPaT messages based on the user needs identified in the Concept of Operations.

Refer to CTI 4501/2 Section 6, Functional Requirements, for functional requirements for MAP messages based on the user needs identified in the Concept of Operations.

Refer to CTI 4501/3 Section 6, Functional Requirements, for the security requirements based on the user needs identified in the Concept of Operations.

Refer to SAE J3258 Section 6, Functional Requirements, for the positioning requirements based on the user needs identified in the Concept of Operations.

7. SYSTEM DESIGN

This section defines the system design guidance based on the requirements identified in the Functional Requirements section. The system design guidance is defined in different CTI 4501/x documents based on the topic.

Refer to CTI 4501 Section 7, System Design, for general design guidance for generic requirements that apply to the connected intersection and all messages based on the user needs identified in the Concept of Operations.

Refer to CTI 4501/1 Section 7, System Design, for general design guidance for functional requirements related to SPaT messages based on the user needs identified in the Concept of Operations.

Refer to CTI 4501/2 Section 7, System Design, for general design guidance for functional requirements related to MAP messages based on the user needs identified in the Concept of Operations.

Refer to CTI 4501/3 Section 7, System Design, for general design guidance for functional requirements related to security requirements based on the user needs identified in the Concept of Operations.

Refer to SAE J3258 Section 7, System Design, for the design guidance for functional requirements related to positioning corrections requirements based on the user needs identified in the Concept of Operations.

8. CONNECTED INTERSECTION TESTING

This section presents a testing framework to verify that an implementation conforms to CTI 4501. This testing framework provides guidance on how to create a verification plan for CTI 4501. The purpose of a verification plan is to confirm that the implementation fulfills all the requirements defined for a connected intersection(s).

The verification plan describes:

- The scope of activities;
- The purpose of each activity;
- The specific verification efforts;
- The resources required to perform the verification activities;
- When the verification activities occurs and where; and
- How to report on the results of the verification activities.

This section presents the elements of a verification plan and the purpose of each element and provides a discussion on what might be included in the scope, with examples of test cases. As CTI 4501 is a guidance document, the contents of this section are NOT standardized test methods, test cases, or test procedures; instead, the contents are EXAMPLES of what might be in a verification plan.

The intended audience of this document are:

- IOO project managers procuring connected intersections, to determine if the system provided conforms to CTI 4501;
- Systems integrators, device vendors, and application providers, to be aware how their products will be tested; and
- Managers and operators of connected intersections, to determine if a connected intersection continues to conform to CTI 4501 during normal operation and after any software or hardware updates.

This section consists of the following sections:

- Introduction: Introduces definitions and the elements of a verification plan.
- Scope: Defines the scope of CTI 4501 conformance testing.
- Planned Activities: Describes when and where the verification activities are to be performed. This plan may also include the test lab environment(s), tools required, and dependencies.
- Test Documentation: Presents the types of test documentation that are to be available or may be produced as a record of the verification activities.

CTI 4501/4 provides the overview and philosophy of testing, while the companion documents provide specific examples based on the focused topics. For example, Section 8 in CTI 4501/1 contains specific examples of test cases for a SPaT message.

8.1 Introduction

Conformance testing is a subset of an overall test framework to verify a connected intersection. See Annex B for a high-level overview of an overall test framework.

8.1.1 Conformance Definition

CTI 4501, 6.2.2.1, Conformance Definition, defines what it means to conform to CTI 4501. In summary, conformance to CTI 4501 means the connected intersection fulfills the minimum requirements to support a RLVW application on an OBU. Recall that the focus of CTI 4501 is the data and performance requirements for the communications interface (the red arrow in Figure 2) between a connected intersection and an OBU/MU. Figure 2 is a graphical depiction of a physical architecture of a connected intersection. The physical elements in the figure are defined in CTI 4501, 5.3.1, Connected Intersection Architecture (and repeated in B.2.1).

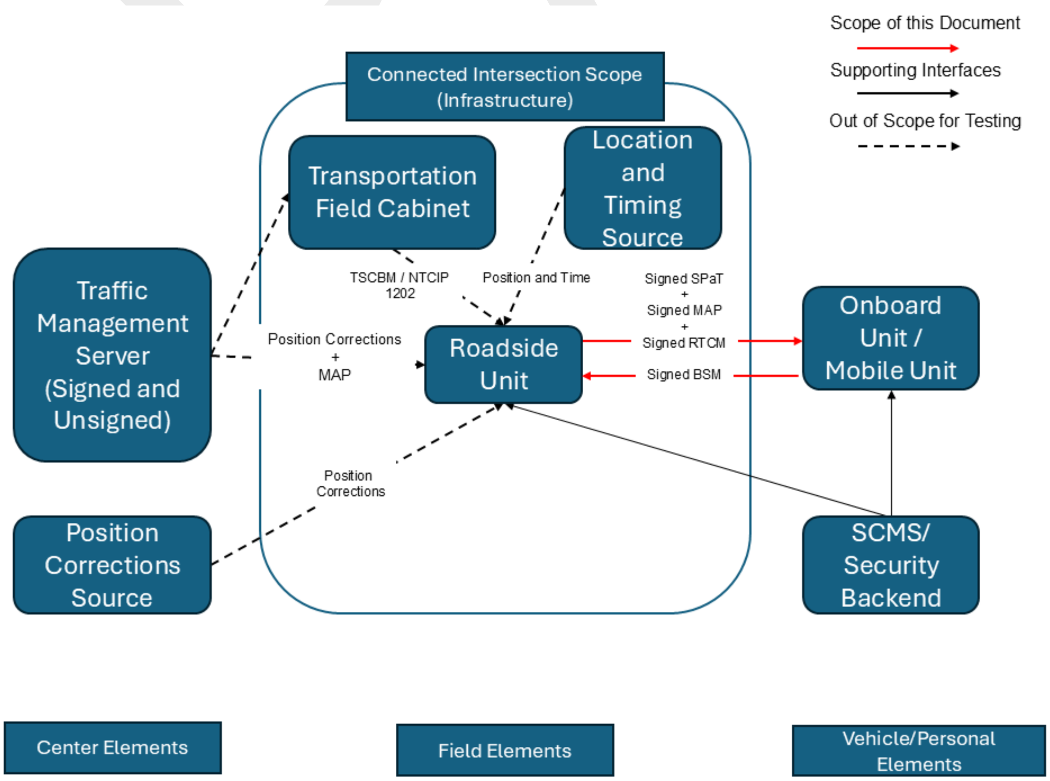

Figure 2 - Connected intersection

A conformant connected intersection must fulfill at least the minimum requirements for CTI 4501, as identified in the NRTM (refer to CTI 4501 Table 5), and is thus likely to be interoperable with other conformant connected intersections. A conformant connected intersection also satisfies the mandatory user needs for a connected intersection and supports all the functional capabilities of an interoperable RLVW application.

Interoperability is defined as the ability of two or more systems or components to exchange information and to use the information that has been exchanged [IEEE Std 610.12, p. 42]. The purpose of communications interface testing as described in this section is to achieve interoperability between a connected intersection and an OBU.

A connected intersection may not be interoperable if it does not conform with CTI 4501. If a connected intersection cannot demonstrate that it conforms with CTI 4501, that intersection might not satisfy the needs of a RLVW application, and an SCMS provider might not provide production certificates to the intersection.

8.1.2 Verification Plan

CTI 4501 is organized following a common system engineering process depicted by the "vee" diagram (see Figure 3). The left side of the "vee" diagram consists of the definition of the systems to be built, and includes the Concept of Operations (Section 5), Requirements (Section 6), and Design and Specifications stage (Section 7).

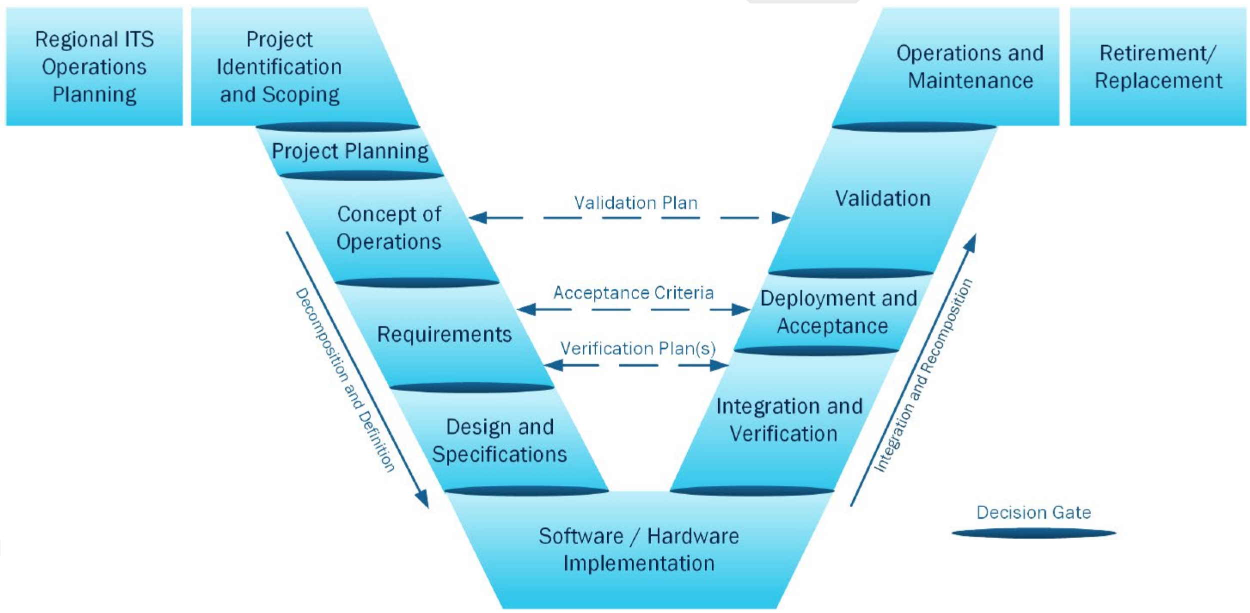

***Figure 3 - Systems engineering "vee" diagram*[1]**

The bottom of the vee diagram encompasses the Software and Hardware Implementation stage, when the hardware and software development activities occur, are monitored, and coordinated. Monitoring is accomplished by a preplanned series of reviews coordinated with the development team. These reviews provide early warning that requirements are deficient or are not being fulfilled by the implementation.

The next stage of the systems engineering process is the Integration and Verification stage, when the system is produced via the integration of the individual components that comprise the system. During this stage, the software and hardware components are individually verified and then integrated to produce higher level assemblies or subsystems. These subsystems are also individually verified before being integrated with other subsystems, until the complete system has been integrated and verified.

The remaining stages on the right side of the vee diagram are described in B.1.2.

[1] Systems Engineering for ITS, FHWA, https://ops.fhwa.dot.gov/seits/

A verification plan is a document that identifies how the requirements for each component, subsystem, and the complete system will be verified. The development of a verification plan is almost always part of a systems engineering effort and is sometimes written along with the requirements specifications. The verification plan answers all the questions of who, what, where, and when concerning the test conduct. A verification plan can also assist a development team to understand the requirements (and design) they are building to, reducing the risk of misinterpretation between agency and manufacturers.

The remainder of Section 8 provides details on the possible contents of a verification plan. When the verification plan is developed (e.g., at the end of the Requirements stage, OR during the Software/Hardware Implementation stage), and by whom (e.g., the systems integrator or the procuring agency), will vary among agencies, based on each agency's policies and procedures (e.g., testing and procurement policies). Example content is also provided throughout the remainder of Section 8.

8.2 Scope

This section defines the scope of CTI 4501 conformance testing. It describes the components and types of testing that will be performed to verify that the implementation under test conforms to CTI 4501.

CTI 4501 identifies various components of a connected intersection, such as TSCs, RSUs, and other components and also depicts other interfaces within the connected intersection. However, CTI 4501 mainly targets the over-the-air message exchange between a connected intersection and the OBU or MU to support RLVW applications.

CTI 4501 provides guidance in three areas:

- Minimum requirements to support a RLVW application, which primarily consists of messages broadcasted by an RSU: SPaT, MAP, and RTCM correction messages;
- Minimum requirements to receive Basic Safety Messages (BSMs) to support AGP; and
- Minimum security requirements across the interface between the connected intersection and the OBU/MU to support a RLVW application.

Figure 2 is a graphical depiction of a physical architecture of a connected intersection. The red arrow in Figure 2 represents the interface between a connected intersection and the applications on the OBUs/MUs. Specifically, the red arrow represents the exchange of data (interface) in the form of digitally signed over-the-air SPaT, MAP, RTCMcorrections, and BSM messages.

CTI 4501 focuses on that interface, defining the minimum communications interface (and performance) requirements needed to support a RLVW application. CTI 4501 conformance testing focuses on the interface from the connected intersection to the OBU/MU only – it verifies that the integrated connected intersection system fulfills the requirements. Thus, the verification activities, and test scope, for CTI 4501 conformance revolves around testing that interface.

The scope of CTI 4501 conformance testing does not extend to all functionalities of the components of a connected intersection, such as a TSC, RSU, traffic cabinet, or the interfaces among these components. Except for SPaT information across the TSC to RSU interface, the requirements for these other interfaces and individual components are not specified in CTI 4501 – those requirements are specified by other standards – and thus are outside the scope of CTI 4501 conformance testing.

For example, NTCIP 1202 standardizes the interfaces with a traffic signal controller, while ATC 5201 and NEMA TS 2 standardize the hardware for a traffic signal controller. While CTI 4501 defines requirements for usage of NTCIP 1202 within a connected intersection, verifying the requirements for that (internal) interface is outside of the scope of CTI 4501 conformance testing.

Agencies aiming to adopt verification of these other components and interfaces might need to merge test approaches from CTI 4501 conformance testing with other tests. These other tests, and guidance to create a test framework for comprehensive functionality testing coverage for a connected intersection, are found in Annex B.

8.2.1 Clarifying Assumptions

The following are assumptions for performing CTI 4501 conformance testing:

- The RSU, GNSS device, and the TSC are operating correctly. For example, the GNSS device is providing accurate position and time information to the connected intersection.

- The RSU has the proper security certificates.

- The TSC has been validated (i.e., the TSC satisfies the mandatory user needs to provide SPaT information to an RSU). (Refer to CTI 4501, 5.4.2.1, Provide Signal Timing Data to an RSU; and CTI 4501, 5.4.2.2, Provide Signal Timing Status to an RSU. Note CTI 4501, 5.4.2.3, RLVW Support, is an optional user need in CTI 4501 Table 5, Needs to Requirements Traceability Matrix.)

- The communications for over-the-air communications between the RSU and the OBU/MU uses LTE-V2X communications.

- Testing the security of the interface is out of scope. However, CTI 4501 conformance testing verifies the use of IEEE Std 1609.2 secured data processing and formats for the messages across the interface under test.

- The Location and Timing Source is typically contained within an RSU. However, the GNSS signal comes from the external environment (e.g., satellite).

- The BSMs received by the connected intersection are valid (i.e., conform to SAE J3161/1).

8.2.2 Conformance Testing Areas

CTI 4501 conformance testing can be categorized into five distinct areas:

- SPaT Message Verification: Describes the scope, testing activities, and test documentation to verify a connected intersection fulfills the CTI 4501 requirements for a SPaT message. Refer to CTI 4501/1 Section 8, Connected Intersection Testing, for more detailed guidance and examples of testing activities and documentation for testing SPaT messages.

- MAP Message Verification: Describes the scope, testing activities, and test documentation to verify a connected intersection fulfills the CTI 4501 requirements for a MAP message. Refer to CTI 4501/2 Section 8, Connected Intersection Testing, for more detailed guidance and examples of testing activities and documentation for testing MAP messages.

- RTCMcorrections Message Verification: Describes the scope, testing activities, and test documentation to verify a connected intersection fulfills the CTI 4501 requirements for a RTCMcorrections message. At the time of publication, a WIP, SAE J3258/1, has been created for a document to provide detailed guidance, example testing activities, and documentation for testing RTCMcorrections messages.

- BSM Verification: Describes the scope, testing activities, and test documentation to verify a connected intersection fulfills the CTI 4501 requirements for a received BSM message. Refer to CTI 4501/1 Section 8, Connected Intersection Testing, for more detailed guidance and examples of testing activities and documentation for testing received BSM messages.

- CI System Security: Describes the scope, testing activities, and test documentation to verify a connected intersection fulfills the CTI 4501 requirements for the messages across the interface between a RSU and an OBU/MU are properly signed. Refer to CTI 4501/3 Section 8, Connected Intersection Testing, for more detailed guidance and examples of testing activities and documentation for testing the security of a connected intersection.

8.2.3 Requirements to Test Case Traceability Matrix (RTCTM)

A requirements to test case traceability matrix (RTCTM) for each of the distinct testing areas (see 8.2.2, Conformance Testing Areas) is provided in the appropriate guidance document (CTI 4501/1 - SPaT Guidance, CTI 4501/2 - MAP Guidance, and CTI 4501/3 - Security Guidance). Each RTCTM is used to:

- Define the relationships between CTI 4501 requirements and specific (verification) test cases;
- Indicate what requirements might need to be tested to verify that an implementation conforms to CTI 4501 for that testing area; and
- Ensure that all the requirements identified for CTI 4501 conformance testing are verified by the verification activities.

Section 8.4, Test Documentation, provides an overview of the different types of documentation, the relationships among each type of documentation, and the importance of each test document. Each requirement to be verified is traced to a test case, which then can be traced to the appropriate stage(s) in the test procedures. A test case is a logical grouping of communications interface and performance requirements that are to be verified together.

NOTE: A test case and test procedures may be called a verification case and verification procedures when used for verification. The same test case and test procedures may be called validation case and validation procedures when used for validation.

Each RTCTM provided in the appropriate guidance document identifies an initial list of example test cases to be performed for CTI 4501 conformance testing for each testing area. To confirm that an implementation fulfills a requirement, the implementation under test shall successfully pass all test cases that trace to that requirement. Collectively, the RTCTMs identify the requirements that must be fulfilled to conform with CTI 4501, and test cases that must be successfully performed to claim conformance with CTI 4501.

Each RTCTM contains the following information:

- Requirement No.: The identifier of the requirement that is being verified by the test case.
- Requirement: A short description of the requirement.
- Test Case Identifier: A unique identifier for the test case(s).
- Test Case Name: A name for the test case(s).
- Verification Method: Identifies the method of verification to be used for the verification case. Valid values are Analysis, Demonstration, Inspection, and Test. The definitions for each method are:
    - Analysis: Verification of system using models, calculations, and testing equipment. This test method is used for a requirement that is fulfilled indirectly through a logical conclusion or mathematical analysis of a result. For example, algorithms for congestion: the designer may need to show that the requirement is met through the analysis of count and occupancy calculations in software or firmware.
    - Demonstration: Manipulation of the system to verify that the results are as planned or expected. This test method is used for a requirement that the system can demonstrate without external test equipment.
    - Inspection: Examination of the system using one of your five senses (auditory, olfactory, tactile, taste, visual). This test method is used for verification through a sensory comparison that the requirement has been satisfied. For example, the Vendor shall provide training on the troubleshooting of the system, including local intersection and central portions.

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

- Mandatory: Identifies if the requirement is mandatory to conform with CTI 4501. A "Y" indicates that the requirement is mandatory and an implementation must successfully pass the test case(s) to claim conformance with CTI 4501. An "N" indicates the requirement is optional, but if the test case is performed, the test case must still pass to be conformant to CTI 4501.

The requirements in each RTCTM should be fulfilled to claim conformance to CTI 4501. Example test cases are also included in each referenced document. The test case details and activities may vary for each agency based on the agency's policies, test methodologies, and preferred test tools.

Refer to CTI 4501/1 Table 7, RTCTM - SPaT Message Verification, for an example RTCTM for SPaT Message Verification.

Refer to CTI 4501/2 Table 6, RTCTM - MAP Message Verification, for an example RTCTM for MAP Message Verification.

Refer to CTI 4501/3 Table 2, RTCTM - Communications Security Verification, for an example RTCTM for Security Verification.

Refer to CTI 4501/1 Table 8, RTCTM - BSM Verification, for an example RTCTM for BSM Verification.

At the time of publication, a WIP, SAE J3258/1 – Test and Validation for GNSS Corrections, has been created for a document to provide detailed guidance, example testing activities, and documentation for testing RTCMcorrections messages. It is expected that the new document will include an example RTCTM.

8.3 Planned Activities

A verification plan must describe the activities needed to verify that a system fulfills the requirement. In this context, the verification plan describes the activities needed to test if a connected intersection conforms to CTI 4501. This section presents some example test methodology concepts, example approaches to testing and conformance, and example test environments.

A verification plan should answer the following questions for the planned activities:[2]

- Does the Verification Plan make clear what needs to happen if a test failure is encountered?
- Does the Verification Plan define the configuration of the hardware, software, and external system needed for each test case?
- Are all applicable requirements traced to a test case in the Verification Plan?
- Does each test case define a realistic and doable test?

[2] Systems Engineering for ITS

8.3.1 Conformance Testing Activities

Annex B presents a test framework for overall and more complete testing of a connected intersection. The test framework in Annex B defines different stages for testing, consistent with the Systems Engineering for ITS (and the vee diagram). Each stage has different goals for testing (see B.2.3). The stages are:

- Software and Hardware Implementation
- Integration and Verification
    - Component Testing
    - Integration Testing
- Deployment and Acceptance
    - Integration Field Testing
    - System Testing
- Validation
    - Burn-in Testing[3]
- Operations and Maintenance
    - Ongoing System Monitoring
    - System Maintenance

Generally, CTI 4501 conformance testing activities, as defined by the RTCTM, are performed at least twice during the life cycle of a connected intersection. The first time is as part of Integration Testing in a controlled test environment, after the components of the connected intersection are combined. CTI 4501 conformance testing activities might be performed only once in the controlled test environment.

The second time is as part of Integration Field Testing after the connected intersection components are installed in its intended location and system integration activities are completed. It is recommended that CTI 4501 conformance testing be performed for every installed connected intersection, to confirm that the hardware and software are properly configured and the connected intersection operates as intended. CTI 4501 conformance testing should be completed and accepted as a requirement for systems acceptance and prior to the start of the validation activities (Burn-in Testing).

A subset (or the complete set) of the conformance testing may be repeated during any other testing stages, as defined by the implementation agency's testing policies and procedures. If CTI 4501 conformance testing is to be performed during other stages of the connected intersection's life cycle, the test environment for each stage should be described in the verification plan. The verification procedures for a specific test case may also be different for each stage.

[3] For vendors = continued checking of verification requirements;
for IOOs = besides long-term verification of requirements, also a means to validate whether the ConOps/User Needs, system design, or requirements were correctly identified and stated. If not, this step is a potential means to identify modifications to an otherwise successfully verified system and to either live with them, to give them to the vendor for potential inclusion in future product updates, or to issue change orders to get them integrated and tested with the delivered system – likely leading to additional testing and another Burn-in testing period.

Each implementation agency should create a matrix to clearly identify the different stages of testing for the agency, and what conformance testing and/or verification activities should occur during each stage of testing.

- CTI 4501/1 Table 9, Verification by Stage - SPaT Message, is an example matrix of when a subset of CTI 4501 conformance testing activities for SPaT messages may be performed or repeated during the different stages of a connected intersection's life cycle.
- CTI 4501/2 Table 7, Verification by Stage - MAP Message, is an example matrix of when a subset of CTI 4501 conformance testing activities for MAP messages may be performed or repeated during the different stages of a connected intersection's life cycle.
- CTI 4501/3 Table 3, Verification by Stage - Security, is an example matrix of when a subset of CTI 4501 conformance testing for Security Verification may be performed or repeated during the different stages of a connected intersection's life cycle.
- CTI 4501/1 Table 10, Verification by Stage - BSM Message, is an example matrix of when a subset of CTI 4501 conformance testing for BSM messages may be performed or repeated during the different stages of a connected intersection's life cycle.

The scope and stages when verification activities may occur will vary based on the agency's testing policies and procedures.

8.3.2 Test Methodology

This section contains example test cases and test methodologies to verify conformance to CTI 4501 in each testing area.

- CTI 4501/1, 8.3.3, Example Test Methodology - SPaT Messages, and SAE J3238/1 provide examples of testing and validation methodologies to verify the accuracy and utility of SPaT to support RLVW applications. CTI 4501/1 presents example test cases, including the test case used for the validation activities in CI Phase 1 (refer to CTI 4502), while SAE J3238/1 details the procedures, steps, and analysis performed for the Utah SMART Grant.
- CTI 4501/2, 8.3.2, Test Methodology - MAP Messages, and SAE J3238/2 provide examples for testing and validation methodologies to verify the accuracy and utility of MAP to support RLVW applications. CTI 4501/2 presents example test cases, including the test case used for the validation activities in CI Phase 1 (refer to CTI 4502), while SAE J3238/2 details the procedures, steps, and analysis performed for the Utah SMART Grant.
- Refer to CTI 4501/3, 8.3.2, Example Test Methodology - Security, for testing and validation methodologies to verify the signatures and profiles for broadcasted messages to support red light violation warnings.
- Refer to SAE J3161/1A for testing and verification methodologies that may be used to verify that an instrument under test (IUT) satisfies the vehicle-level requirements specified in SAE J3161/1.
- At the time of publication, a WIP, SAE J3258/1 – Test and Validation for GNSS Corrections, has been created for a document to provide detailed guidance, example testing activities, and documentation for testing RTCMcorrections messages. It is expected that the new document will include an example RTCTM.

8.3.3 Test Environment

This section describes how to specify test environments to verify conformance to CTI 4501. The test environment specification should describe the necessary and desired properties of the test environment, such as what hardware is necessary, what software tools will be used, what data is available, and the necessary physical characteristics of the test facilities (such as a test bench, chairs, manuals, or documentation that is to be readily available).

For example, the SPaT verification plan must outline the test environment to establish a foundation for thorough and uniform testing, enabling the simulation of real-world traffic scenarios. Figure 4 provides an example of the laboratory test environment created for SPaT message testing in CI Phase 1.

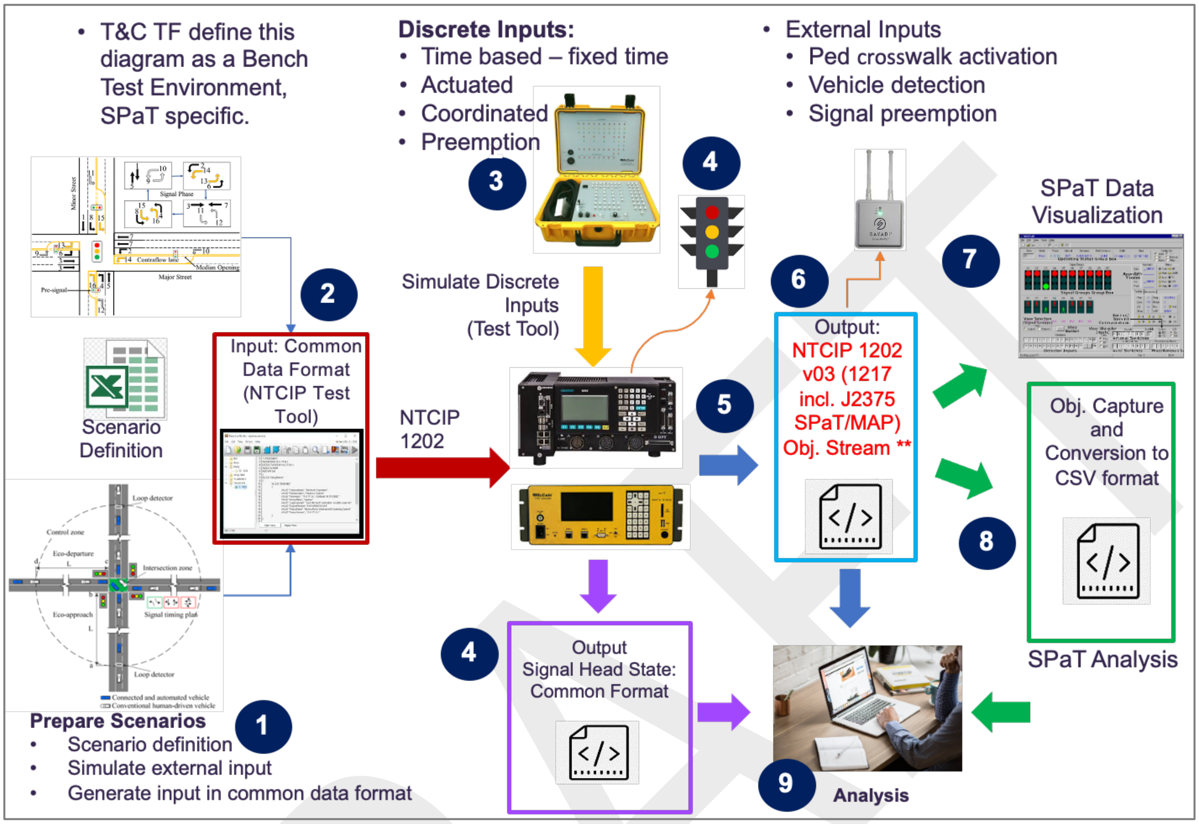

Figure 4 - Example test environment for SPaT testing

The numbers reflect potential steps to be described in a test procedure. The test procedures described here were used to validate the SPaT messages during a validation phase of CTI 4501 v01, which took place between April and September of 2021.

1. Prepare operational test scenarios.
2. NTCIP Test tool test input (operational scenario) to the Controller (e.g., from laptop). Note: For CI Phase 1, SPaT data was provided in TSCBM format.
3. Test tool (e.g., suitcase tester) generates discrete inputs to Controller, e.g., pedestrian crosswalk activation, vehicle detection.
4. Controller output to Signal Head and to a file (CSV format).
5. Simultaneous with step 4, Controller outputs NTCIP 1202 v03 (SPaT information) for RSU.
6. Controller outputs from step 5 are captured through RSU's over-the-air radio transmission in a PCAP file and then converted to JSON CSV file.
7. Simultaneous with Step 6, a Visualization Tool shows Signal State and Controller Output destined to the RSU.
8. Test tool (e.g., Texas Transportation Institute Test Tool) converts byte-oriented SPaT information or NTCIP 1202 v03 packets to a CSV file.
9. The output data captures from Controller are time synchronized to verify controller outputs are correct for a given set of initial inputs defined in steps 1, 2, and 3.

In CI Phase 2 of the CTI 4501 project, the SPaT verification process was enhanced to accurately obtain the signal phase status as reported by the signal controller, thereby establishing the ground truth. A Data Acquisition Tool (DAT) was created to connect with the Synchronous Data Link Control (SDLC) for serial data frames within the traffic cabinet. Furthermore, the DAT records the broadcast messages for SPaT verification, enabling the capture of actual signal phase statuses in real-world scenarios. Figure 5 illustrates traffic cabinet DAT concept.

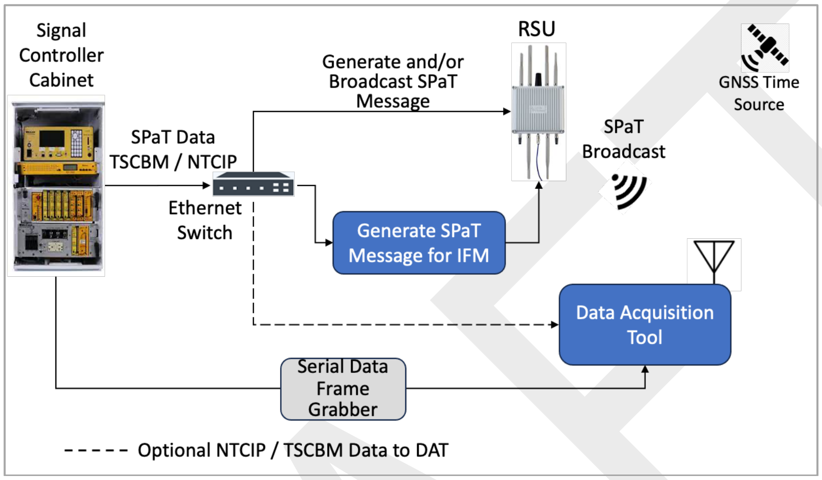

Figure 5 - Example traffic cabinet data acquisition tool for SPaT

8.4 Test Documentation

Documenting test results during CTI 4501 conformance testing is crucial for a connected intersection for several reasons:

- It serves as proof that the connected intersection has been implemented correctly.
- It aids in monitoring the connected intersection and identifying any anomalies in its behavior from previously documented results.
- It provides a baseline for the connected intersection following modifications or outages.
- It is a necessary step for acquiring security certifications from a certificate authority.

8.4.1 Test Documentation Overview

This section provides an introduction to test documentation, which describes a set of basic test documents that are associated with testing, such as verification and validation. Test documentation, as described in IEEE Std 829, IEEE Standard for Software and System Test Documentation, includes the following:

- Test Plans
- Requirements Verification
    - Test Cases
    - Test Procedures
- Test Execution
    - Test Logs
    - Test Anomaly Reports
- Test Summary Report

Figure 6 illustrates the relationships of the various test documentations described above.

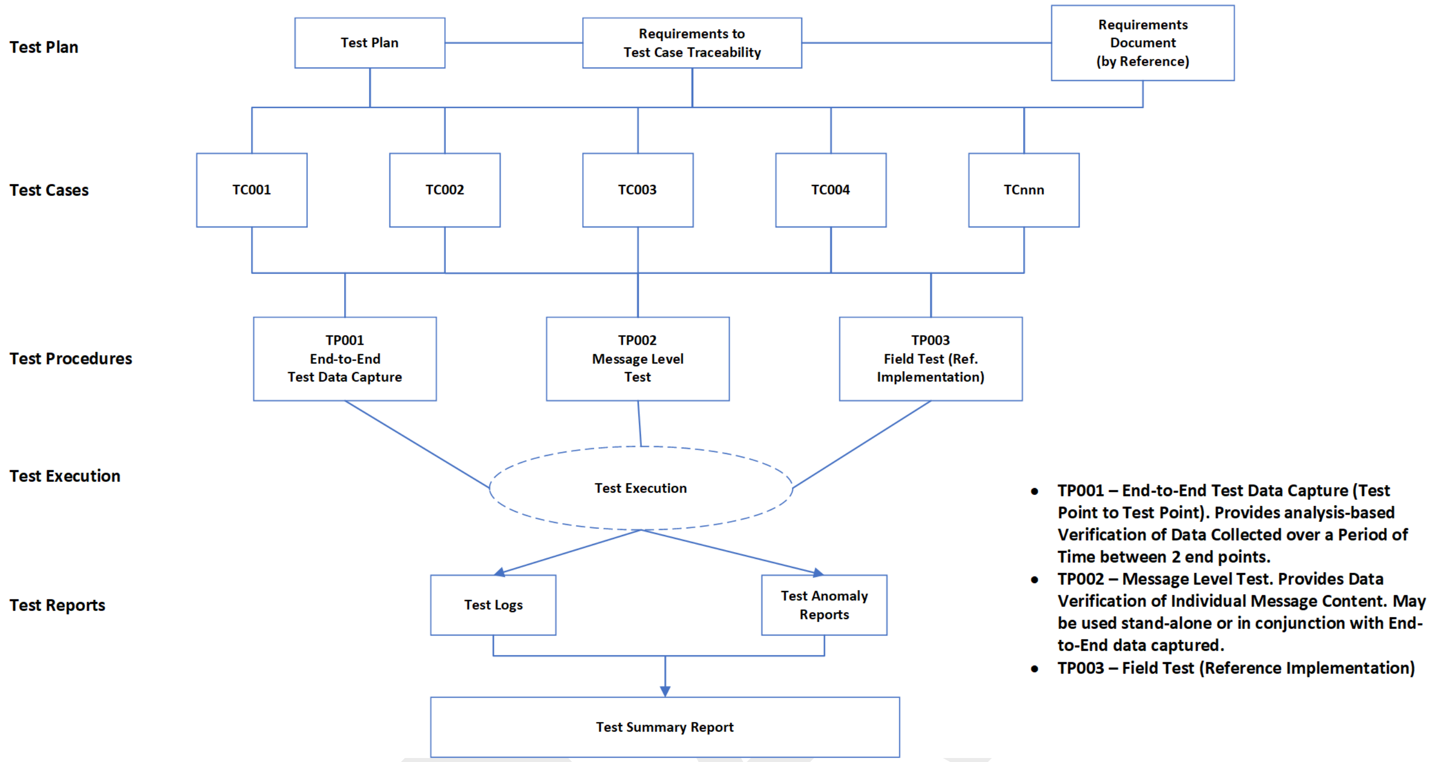

Figure 6 - Test documentation relationships

8.4.2 Test Plans

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

The test plan documents the approach to use to verify each of the system and subsystem requirements. The plan identifies the test cases to verify each requirement and general processes to use to execute the test cases and deal with verification issues. Test procedures elaborate each test case and specify the step-by-step actions and expected responses.

For CTI 4501 conformance testing, the test plan is called a verification plan.

A test plan shall contain the following sections and structure.

- Test Items: Identifies the test items (interfaces, modules, software, or system) that are the objects of testing.
- Features to Be Tested: Identifies all software product or software-based system features and combinations of software or system features to be tested.
- Features Not to Be Tested: Identifies all features and known significant combinations of features that will not be tested and the rationale for exclusion.
- Test Coverage: Specifies the requirement(s) for test coverage. Test coverage is an indication of the degree to which the test item has been reached or "covered" by the test cases.

- Item Pass/Fail Criteria: Specifies the criteria to be used to determine whether each test item has passed or failed testing.

- Requirements to Test Case Traceability Matrix: A matrix used to verify that test cases are developed for each requirement, at least once. This matrix is used to assist with test coverage assessment.

- Roles and Responsibilities: Identifies the individuals or groups responsible for managing, designing, preparing, executing, witnessing, checking results, and for resolving the anomalies found.

- Resources Summary: Summarizes the test resources, including staffing, facilities, tools, and special procedural requirements (e.g., security, access rights, and documentation control).

- Test Schedule: Describes the test activities within the project life cycle and milestones. Summarizes the overall schedule of the testing tasks, identifying where task results feed back to the development, organizational, and supporting processes (e.g., quality assurance and configuration management).

- Document Procedures and History: Specifies the means for identifying, approving, implementing, and recording changes to the test plan.

The test plan should also include a section on suspension criteria and resumption requirements. This section identifies the procedures in the event of a test case failure. Examples of suspension and resumption requirements include:

- All test cases are unrelated and do not depend on each other. If a test case fails, the performance of another test case may commence.

- If a test case fails because a parameter was not set properly (for example, a password or username has been misspelled), the test case that has failed may be run again.

- If an anomaly is likely to be caused by a problem that requires a software modification, the test case remains as failed until the software modification is made.

- Verification testing is expected to occur over several days, but each test case is expected to be completed within a day. If a test case is not completed within a day, verification activities may stop and recommence the following day.

- Procedures for approving last-minute changes to the procedures.

- The processes for handling a failure, including recording of critical information, determination of whether to stop the verification, restart, or skip a procedure, resolution of the cause of a failure (e.g., fix the software, reset the system, and/or change the requirements), and determination of the reverification activities necessary as a result of the failure.

8.4.3 Test Cases

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

A test case is expanded into test procedures that define a series of steps that will be performed to verify each component, subsystem, or system against its requirements. For efficiency, test cases may be used to verify multiple requirements.

A test case shall contain the following sections and structure.

- Test Case Identifier: Describes the unique identifier needed by each test case so that it can be distinguished from all other test cases. An automated tool may control the generation of the identifiers.

- Inputs: Specifies each input required to execute each test case. Some inputs will be specified by value (with tolerances where appropriate), whereas others, such as constant tables or transaction files, will be specified by name.

- Outcomes: Specifies all outputs and the expected behavior (e.g., response time) required of the test items and provides the exact value(s) (with tolerances where appropriate).

- Feature Pass/Fail Criteria: Specifies the criteria to be used to determine whether the feature or feature combination has passed or failed.

- Intercase Dependencies: Lists the identifiers of test cases that must be executed prior to this test case. The test case shall summarize the nature of the dependencies. The test case may also describe all of the necessary initial conditions and setup before executing the test case. If test cases are documented (in a tool or otherwise) in the order in which they need to be executed, the Intercase Dependencies for most or all of the cases may not be needed.

Example test cases are found in CTI 4501/1, 8.3.3.1, and CTI 4501/2, 8.3.2.1. Additional fields can be added depending on an agency's test policies and procedures.

8.4.4 Test Procedures

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

Test procedures define the step-by-step procedure to conduct the testing and must be traceable to the test plan.

The components of a test procedure are:

- Test Procedure Identifier: Describes the unique identifier needed by each test procedure so that it can be distinguished from other test procedures.

- Test Case References: References to relevant sections of any applicable test item documentation (e.g., references to test cases to be performed).

- Requirements Verification Methods: Identify a method of verification to be applied in the test procedure. It is generally accepted that there are four methods of requirements verification. See Verification Method in 8.2.3.

- Procedure Descriptions: Contain high level descriptions of the test procedures.

- Procedure Steps: Ordered description of the steps to be taken by each participant.

Each step may also indicate the expected outputs, what requirement the step traces to, and what requirement is verified by the successful completion of the step.

Example test procedures for testing SPaT and MAP messages are found in SAE J3238/1 and SAE J3238/2, respectively.

8.4.5 Test Logs

A detailed record documenting the activities that are executed during testing. A test log shall contain the following sections and structure.

- Description: Contains general information that applies to all entries in the log (exceptions can be specifically noted in a log entry). The following information may be considered:
  - Identify the items being tested
  - Date and time of start and stop
  - Name of the individual running the test
  - Any issue that causes testing to halt
- Activity and Event Entries: Records activities/events for each relevant detail, including the beginning and end of activities, and the occurrence date and time along with the identity of the author. Information may include:
  - Context. Such as Test Case Identifier or the Test Procedure Identifier.
  - Start Date/Time.
  - Procedure Results. For each execution, create a record of the results (manually or automated by a tool).
  - Test Case Pass/Fail.
  - Anomaly Report Identifiers. Record the identifier of each test Anomaly Report.

Example test logs for SPaT messages are found in SAE J3238/1.

8.4.6 Test Anomaly Reports

A record of anomalies observed during testing activities. Anomalies are any user activity that is unexpected or sufficiently different from historical activity, and any activity that results in a failed test case or a failed requirement. A test anomaly report shall contain the following sections and structure.

- Test Anomaly Report Identifier: Each test anomaly report shall have unique identifiers.
- Test Anomaly Report – Date Anomaly Discovered: Records the date and time that the anomaly was first identified.
- Test Anomaly Report – Context: Identifies the test items involved indicating their version/revision level. References to the appropriate Test Procedure, Test Case, and Test Log may be supplied.
- Test Anomaly Report – Description of the Anomaly: Contains a description of the anomaly. Indicate whether the anomaly is reproducible, and provide enough information to make it reproducible if it is.
- Test Anomaly Report – Assessment of Urgency: An evaluation of the need for an immediate repair because of the impact of the anomaly.
- Test Anomaly Report – Description of the Corrective Action: Summarizes the activities during the corrective action taken to resolve the reported anomaly. It may include the time, effort, and risk required for the fix(es), with the actual time and effort added after the fix is completed.
- Test Anomaly Report – Conclusions and Recommendations: Specifies any recommendations for changes to the development and/or testing processes and documentation that would help to prevent this kind of anomaly in the future. This may include identification of the source or injection point of the anomaly.

Anomalies during CTI 4501 conformance testing that may be reported include:

- Any erroneous exchanged data (e.g., bad value, bad formatting)
- Configuration Error
- System Documentation
- Operator Error

8.4.7 Conformance Summary Report

A document summarizing the results of the testing activities and provides evaluations and recommendations based on the results, the conformance summary report provides critical information about the conduct of the testing activities and should provide evidence that the connected intersection fulfills the requirements and identify any corrective actions that were recommended or taken due to the verification process.

For example, the report should describe in detail the resolution of every test anomaly encountered during testing.

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

- Conformance Summary: Identifies the cumulative result of testing (Pass/Fail) as to whether a Connected Intersection is conformant with CTI 4501.
- Summary of Testing Activities: Contains an executive-level summary of all test activities performed in support of this release, increment, or version. The activities identified in this section of the report should correspond to the test activities described in the Test Plan.
- Summary of Testing Task Results: Contains an executive-level summary of all testing tasks performed in support of this release, increment, or version. The tasks identified in this section of the report should correspond to the test tasks described in the Test Plan. This section also references Summary of Pass/Fail Results.
- Summary of Anomalies and Resolutions: Contains a categorized summary of anomalies discovered during testing performed in support of this release, increment, or version.
- Summary of Pass/Fail Results: Organized to include Test Item, Test Case, Test Procedure or Requirement.

The conformance summary report should also include the date, time, and location each test case was started and completed, the names of the participants and witnesses present, if test procedures were completed or skipped, any anomalies observed during testing, (e.g., system was reset, software modification, configuration modification, etc.), and if the performance of the test case passed or failed. Space may also be included on the summary report to allow the owner agency representative signatures and dates. The signatures on the summary report indicate the test was performed and witnessed and whether a test case was passed or failed.

9. NOTES

9.1 Revision Indicator

A change bar (l) 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 - TESTING RESOURCES [INFORMATIVE]

This annex contains a list of resources for testing.

A.1 EXISTING TEST DOCUMENTATION

Many of these references listed in Table A1 are available from USDOT or CAMP. See references in Section 2.

Table A1 - Existing test documentation

Document Name, Date	Comment	Sponsor	Test Plan	Test Procedures	Test Cases	Test Log	Test Report
Test Plan for Connected Vehicle (CV) Pilots Phase 2 Interoperability Testing, May 15, 2018	Provided by J. Anderson, also D. Benevelli	FHWA	X	Data Collection	X	X	
Connected Vehicle Pilots Phase 2 Interoperability Test Test Report, November 9, 2018	Provided by J. Anderson	FHWA	X		X		X
Test Procedure for Verifying SPaT and MAP Messages, September 18, 2019	Provided by J. Parikh	CAMP		X			
SPaT Challenge Verification Document, October 30, 2017	Provided by J. Parikh	CAMP		X			
Test Readiness Review Checklist	Provided by J. Anderson. Useful for tracking/conducting test readiness review (TRR) which is the final go/no-go decision for conducting the test.	FHWA	X	X			
Interoperability Test Notebook	Provided by J. Anderson. Used to create physical notebooks for data collection and tracking of each test.	FHWA				X	
Interoperability Test Compiled Notebook	Provided by J. Anderson. Spreadsheet format to consolidate information collected from the notebooks.	FHWA				X	
Actual Run Order and Start Times	Provided by J. Anderson. Consolidated list of all test runs and in what order.	FHWA				X	
DRAFT Connected Vehicle Deployment Environment, August 2020	Provided by J. Parikh	CAT Coalition	X				

A.2 EXAMPLE USAGE OF A TEST TOOL

The section contains an example usage of an OBU-based test tool, to verify that a broadcasted SAE J2735 SPaT and MAP message conforms with the requirements of CTI 4501.

Figure A1 shows the OBU-based Test Tool in relation to the project scope, indicated by the red arrow at left, and the OBU Test Tool log file at right:

Figure A1 - Example testing scope for OBU-based test tool

A.2.1 Description of OBU-Based Test Tool JSON Log

The OBU-Based Test Tool's log file is a comma-delimited text file with each record containing four parts. Records in the log file are separated (terminated) with a line feed.

The four parts of the OBU-Based Test Tool Log File are described below:

- TimeStamp: Epoch time to indicate message received time by the OBU.
- MessageID: The SAE J2735 MessageID to indicate message type: 18=MAP, 19=SPaT.
- Message: An SAE J2735 SPaT or SAE J2735 MAP message represented in JSON Encoding Rules format. The JSON itself does not contain any line feeds or extra spaces. Because JSON contains commas and quotation characters, it is necessary to begin and end the JSON with a single-quote character.
- SignedMessageIndicator: 0 represents unsigned message, 1 represents signed message.

An example log file containing data format including the SPaT messages in JSON and imported into MS Excel is shown in Figure A2.

A	B	C							D
1614109658855	19	'{"messageId":19	value:{"inter	revision:52	status:"0000	moy:78440	timeStamp:3	states:[{"sig	0
1614109658860	19	'{"messageId":19	value:{"inter	revision:53	status:"0000	moy:78440	timeStamp:3	states:[{"sig	0
1614109658865	19	'{"messageId":19	value:{"inter	revision:54	status:"0000	moy:78440	timeStamp:3	states:[{"sig	0
1614109658901	19	'{"messageId":19	value:{"inter	revision:55	status:"0000	moy:78440	timeStamp:3	states:[{"sig	0
1614109658905	19	'{"messageId":19	value:{"inter	revision:56	status:"0000	moy:78440	timeStamp:3	states:[{"sig	0
1614109658908	19	'{"messageId":19	value:{"inter	revision:57	status:"0000	moy:78440	timeStamp:3	states:[{"sig	0
1614109658912	19	'{"messageId":19	value:{"inter	revision:58	status:"0000	moy:78440	timeStamp:3	states:[{"sig	0
1614109658915	19	'{"messageId":19	value:{"inter	revision:59	status:"0000	moy:78440	timeStamp:3	states:[{"sig	0
1614109658919	19	'{"messageId":19	value:{"inter	revision:60	status:"0000	moy:78440	timeStamp:3	states:[{"sig	0
1614109658922	19	'{"messageId":19	value:{"inter	revision:61	status:"0000	moy:78440	timeStamp:3	states:[{"sig	0
1614109658926	19	'{"messageId":19	value:{"inter	revision:62	status:"0000	moy:78440	timeStamp:3	states:[{"sig	0
1614109658929	19	'{"messageId":19	value:{"inter	revision:63	status:"0000	moy:78440	timeStamp:3	states:[{"sig	0
1614109658933	19	'{"messageId":19	value:{"inter	revision:64	status:"0000	moy:78440	timeStamp:3	states:[{"sig	0

Figure A2 - Example log file output

It should be noted that the JSON, shown in column C, is not a complete message. The complete message is a long string.

A.2.2 OBU-Based Test Tool JSON Log - Example SPaT Message

An exploded view of the SPaT JSON contained in the log file is shown in Figure A3.

It should be noted that, to reduce the logged JSON file size, there are no spaces in a record. Each record in the file ends with linefeed (new line). A log file contains both SPaT and MAP messages as being broadcast by an RSU. A post processing software separates the SPaT and MAP messages and saves them in separate files for parsing JSON and message processing for each intersection.

Example: OBU Test Tool logged data record for a SPaT message. The logged SPaT messages file contains all received SPaT messages.

1610557070717,19,'{"messageId":19,"value":{"intersections

```
{
  "timestamp": 1610557070717,    <-- Epoch Time
  "messageId": 19,    <-- Msg ID
  "value": {
    "intersections": [    <-- Example SPaT message in JSON
      {
        "id": {
          "id": 173
        },
        "revision": 89,
        "status": "0000",
        "moy": 19230,
        "timeStamp": 45484,
        "states": [
          {
            "signalGroup": 2,
            "state-time-speed": [
              {
                "eventState": "protected-Movement-Allowed",
                "timing": {
                  "minEndTime": 34654,
                  "maxEndTime": 35244
                }
              }
            ]
          },
          {
            "signalGroup": 4,
            "state-time-speed": [
              {
                "eventState": "stop-And-Remain",
                "timing": {
                  "minEndTime": 34711,
                  "maxEndTime": 35301
                }
              }
            ]
          },
          {
```

Figure A3 - Log file entry SPaT JSON encoding rules

```
          "signalGroup": 5,
          "state-time-speed": [
            {
              "eventState": "stop-And-Remain",
              "timing": {
                "minEndTime": 34654,
                "maxEndTime": 34654
              }
            }
          ]
        },
        {
          "signalGroup": 6,
          "state-time-speed": [
            {
              "eventState": "protected-Movement-Allowed",
              "timing": {
                "minEndTime": 34700,
                "maxEndTime": 35380
              }
            }
          ]
        }
      ]
    }
  ]
},
"status": 0
}
```


Figure A3 - Log file entry SPaT JSON encoding rules (continued)

Important: The logged messages in JSON above must reflect the same names as specified in the ASN.1 description of an SAE J2735 SPaT message. An example of the ASN.1 for SAE J2735 is shown below.

EXAMPLE 1: Snippet of ASN.1 for LaneAttributes-Vehicle:

```
LaneAttributes-Vehicle ::= BIT STRING {

  -- With bits as defined:

  isVehicleRevocableLane    (0),

                    -- this lane may be activated or not based

                    -- on the current SPaT message contents

                    -- if not asserted, the lane is ALWAYS present

  isVehicleFlyOverLane      (1),

                    -- path of lane is not at grade
```

```
  hovLaneUseOnly          (2),
  restrictedToBusUse      (3),
  restrictedToTaxiUse     (4),
  restrictedFromPublicUse (5),
  hasIRbeaconCoverage     (6),
  permissionOnRequest     (7) -- e.g., to inform about a lane for e-cars
  } (SIZE (8,...))
```

EXAMPLE 2: Snippet of ASN.1 for TimeChangeDetails:

```
TimeChangeDetails ::= SEQUENCE {
  startTime   TimeMark          OPTIONAL,
              -- When this phase 1st started
  minEndTime  TimeMark,
              -- Expected shortest end time
  maxEndTime  TimeMark          OPTIONAL,
              -- Expected longest end time
  likelyTime  TimeMark          OPTIONAL,
              -- Best predicted value based on other data
  confidence  TimeIntervalConfidence OPTIONAL,
              -- Applies to above time element only
  nextTime    TimeMark          OPTIONAL
              -- A rough estimate of time when
              -- this phase may next occur again
              -- used to support various ECO driving power
              -- management needs.
  }
```

EXAMPLE 3: Snippet of ASN.1 for TimeMark:

```
TimeMark ::= SEQUENCE {
   year        Year,        -- BCD coding of A.D.    2 octets
   month       Month,       -- BCD coding of Month,  1 octet
   day         Day,         -- BCD coding of Day,    1 octet
   summerTime  SummerTime,
   holiday     Holiday,
   dayofWeek   DayOfWeek,
   hour        Hour,        -- BCD coding of Hour,   1 octet
   minute      Minute,      -- BCD coding of Minute, 1 octet
   second      Second,      -- BCD coding of Second, 1 octet
   tenthSecond TenthSecond  -- units of 100 millisecond, 1 octet
}
```

For complete details, refer to SAE J2735_201603 Final ASN specification.

A.2.3 OBU-Based Test Tool JSON Log - Example MAP Message

The following example shows test tool logged data for a MAP message.


```
{
  "timestamp": 1610557070790,
  "messageId": 18,
  "value": {
    "msgIssueRevision": 0,
    "layerType": "intersectionData",
    "layerID": 1,
    "intersections": [
      {
        "id": {
          "id": 173
        },
        "revision": 1,
        "refPoint": {
          "lat": 422837517,
          "long": -837109988,
          "elevation": 205
        },
        "laneWidth": 306,
        "laneSet": [
          {
```


Epoch Time

Msg ID

Example MAP Message in JSON

Figure A4 - Example log file entry with MAP JSON encoding rules

```
        "laneID": 3,
        "ingressApproach": 1,
        "laneAttributes": {
          "directionalUse": "80",
          "sharedWith": "1d80",
          "laneType": {
            "vehicle": {
              "value": "01",
              "length": 8
            }
          }
        },
        "maneuvers": "4000",
        "nodeList": {
          "nodes": [
            { "delta": { "node-XY3": { "x": 802, "y": -1568 } } },
            { "delta": { "node-XY1": { "x": 6, "y": -11 } } },
            { "delta": { "node-XY2": { "x": 380, "y": -759 } } },
            { "delta": { "node-XY3": { "x": 601, "y": -1196 } } },
            { "delta": { "node-XY1": { "x": 281, "y": -465 } } },
            { "delta": { "node-XY1": { "x": 250, "y": -407 } } },
            { "delta": { "node-XY1": { "x": 281, "y": -437 } } },
            { "delta": { "node-XY2": { "x": 464, "y": -636 } } },
            { "delta": { "node-XY3": { "x": 1343, "y": -1203 } } }
          ]
        },
        "connectsTo": [
          {
            "connectingLane": {
              "lane": 9,
              "maneuver": "4000"
            },
            "signalGroup": 5
          }
        ]
      },
      {
        "laneID": 4,
        "ingressApproach": 1,
        "laneAttributes": {
          "directionalUse": "80",
          "sharedWith": "1d80",
          "laneType": {
            "vehicle": {
              "value": "01",
              "length": 8
            }
          }
```


Figure A4 - Example log file entry with MAP JSON encoding rules (continued)

```
            },
            "maneuvers": "8000",
            "nodeList": {
              "nodes": [
                { "delta": { "node-XY3": { "x": 1141, "y": -1417 } } },
                { "delta": { "node-XY2": { "x": 430, "y": -850 } } },
                { "delta": { "node-XY2": { "x": 474, "y": -933 } } },
                { "delta": { "node-XY2": { "x": 563, "y": -931 } } },
                { "delta": { "node-XY2": { "x": 440, "y": -786 } } },
                { "delta": { "node-XY2": { "x": 652, "y": -957 } } },
                { "delta": { "node-XY2": { "x": 708, "y": -808 } } },
                { "delta": { "node-XY2": { "x": 675, "y": -719 } } },
                { "delta": { "node-XY3": { "x": 982, "y": -1036 } } },
                { "delta": { "node-XY2": { "x": 919, "y": -920 } } },
                { "delta": { "node-XY3": { "x": 1494, "y": -1286 } } },
                { "delta": { "node-XY3": { "x": 1735, "y": -1456 } } },
                { "delta": { "node-XY4": { "x": 2161, "y": -1768 } } },
                { "delta": { "node-XY3": { "x": 1676, "y": -1430 } } },
                { "delta": { "node-XY3": { "x": 1796, "y": -1484 } } },
                { "delta": { "node-XY4": { "x": 2189, "y": -1708 } } },
                { "delta": { "node-XY4": { "x": 2342, "y": -1882 } } },
                { "delta": { "node-XY4": { "x": 2307, "y": -1705 } } },
                { "delta": { "node-XY4": { "x": 2394, "y": -1614 } } },
                { "delta": { "node-XY3": { "x": 1519, "y": -1056 } } }
              ]
            },
            "connectsTo": [
              {
                "connectingLane": {
                  "lane": 8,
                  "maneuver": "8000"
                },
                "signalGroup": 2
              }
            ]
          },
          ...
          // Additional lane definitions (laneID 5 to laneID 11) go here
        ]
      }
    ]
  },
  "status": 0
}
```

Signed Msg Indicator

Figure A4 - Example log file entry with MAP JSON encoding rules (continued)

Similar to the SPaT message, the MAP message also contains epoch time, message id, MAP message (in italics), and signed message indicator.

ANNEX B - CONNECTED INTERSECTION TESTING FRAMEWORK [INFORMATIVE]

Annex B presents a testing ***framework*** to verify and validate a connected intersection through its operational life cycle: from when the connected intersection is first procured, to acceptance testing, and through continuous monitoring during its operation and maintenance until it is retired or replaced.

Testing is an important phase of a complex system such as a connected intersection. A connected intersection is composed of various independent components that must work together as a system to satisfy the selected user needs and specified requirements. IEEE Std 829 defines the purpose of testing as:

> to help the development organization build quality into the… system during the life cycle processes and to validate that the quality was achieved. The test process determines whether the products of a given life cycle activity conform to the requirements of that activity, and whether the product satisfies its intended use and user needs.[4]

The overall goal of testing is to ensure system reliability, performance, safety, and compliance with specifications to meet selected user needs throughout its operational life cycle. A test framework, and the testing processes that comprise the test framework, is crucial to ensure consistency and compatibility of connected intersections, which lead to more cost-effective support and quicker adoption of connected vehicle safety systems.

This annex provides a high-level overview of testing activities. This annex does not delve into detailed testing procedures or test planning, such as testing tasks, personnel responsibilities, timeline, etc. This annex is a supplement to Section 8, Connected Intersection Testing. While Section 8 describes how to verify conformance to CTI 4501, this annex is written with an eye for a prospective IOO building and validating a connected intersection, and considering what testing policies and procedures are necessary to continuously validate the connected intersection, including when a change is made to the connected intersection. As such, CTI 4501 conformance testing is a subset of an overall test framework to validate a connected intersection.

This annex consists of the following subsections:

- **Introduction**, which provides an overview of where testing fits in the operational life cycle of a connected intersection, what it means to test for CTI 4501 conformance, and what a test framework is.

- **Developing a Test Framework**, which describes the different components, types of testing, and test stages that comprise a test framework for a connected intersection. This subsection also provides examples of each type of testing.

Annex B is intended for the following stakeholders:

- For systems integrators, application developers, and device vendors to understand how to verify and validate the individual components of a connected intersection and the connected intersection itself; and to understand the selected user needs of the procuring IOO;

- For transportation operators to understand how a connected intersection is intended to function and its outputs;

- For maintenance personnel to determine what testing is to be performed while the system is in operation and before the system is to be placed back into operations; and

- For security certificate providers, to understand how an IOO continuously verifies and validates that the quality of the system, as defined by the requirements and user needs, is maintained so production security certificates can be provided.

[4] Reprinted with permission from IEEE. Copyright IEEE 2008. All rights reserved.

B.1 INTRODUCTION

The necessity for a formal test framework by an IOO arises from the potential risks associated with a connected intersection providing inaccurate, erroneous, or untimely data to an OBU or a mobile device. When a connected intersection operates in Normal mode (refer to CTI 4501, 6.3.5.3.1, Support Normal Mode) and transmits messages signed with SCMS certificates, the receiving applications place trust in this data and may use it to issue safety warnings. Operating a connected intersection without formal testing has a higher risk of providing incorrect data or failing to fulfill the selected requirements. This could lead to unintended consequences within the receiving applications and could lead to increased costs to maintain system in operation, hence emphasizing the importance of thorough system testing.

From an IOO perspective, the primary purpose of testing is two-fold:

- How an IOO may test a connected intersection for conformance to CTI 4501 (verification). This is accomplished by verifying that all the mandatory requirements in CTI 4501 Section 6 are fulfilled by the connected intersection delivered to the IOO (see Section 8).

- How an IOO may develop a test framework to validate a connected intersection. Validation confirms that the connected intersection satisfies the mandatory user needs of CTI 4501 once the connected intersection is deployed and operational in its intended environment.

While successful verification confirms that a connected intersection conforms with CTI 4501, this may also be a required step for obtaining SCMS security certificates needed for the intersection to function in Normal mode.

The test framework presented here is a blueprint for an overall testing program for IOOs deploying connected intersections. The test framework includes CTI 4501 conformance testing (see Section 8), but it only specifies a subset of the requirements that comprise a connected intersection – specifically, CTI 4501 conformance testing focuses only on the requirements between a connected intersection and one of the potential CV applications, namely the RLVW application, running on an OBU. There are also many other requirements for a connected intersection not specified in CTI 4501, such as functional, hardware, and environmental requirements, and requirements for applications other than a RLVW application. These other requirements are the focus of this annex.

The test framework presented describes test activities to provide objective data and conclusions about software and system quality. This feedback can include anomaly identification, performance measurement, and identification of potential quality improvements for expected operating conditions across the full spectrum of the software-based systems and their interfaces. Early feedback allows the development organization to modify the products in a timely fashion and thereby reduce overall project and schedule impacts. Without a proactive approach, anomalies and associated changes are typically delayed to discovery and resolution later in the schedule, likely resulting in greater costs and schedule delays.

B.1.1 Overview

This annex presents an overall testing framework for a connected intersection, from describing the subsystems (components) of a connected intersection, followed by the types of testing that should be considered, ending with the stages of testing that should be performed during the entire life cycle of the connected intersection; starting with initial testing of the first component until the connected intersection is taken out of service.

This annex contains high-level recommendations on what should be part of an agency's testing program for deploying, operating, and maintaining a connected intersection. Where a standard, technical report, or example exists for testing, this framework references those documents so they can be used to develop the IOO's testing program, if appropriate.

B.1.2 Testing in the Systems Engineering Process

CTI 4501 is organized following a common system engineering process depicted by the "vee" diagram below. The left side of the "vee" diagram consists of the definition of the system to be built, and includes the Concept of Operations (refer to CTI 4501 Section 5), Requirements (refer to CTI 4501 Section 6), and the System Design (refer to CTI 4501 Section 7). Testing activities and required testing documentation may also be defined during the execution of these phases, but they must be defined prior to system acceptance. Additionally, testing tools, including those needed during the Operations and Maintenance period, must be identified and included in the testing activities (whether early as a "may" or later as a "must" tool identification activity).

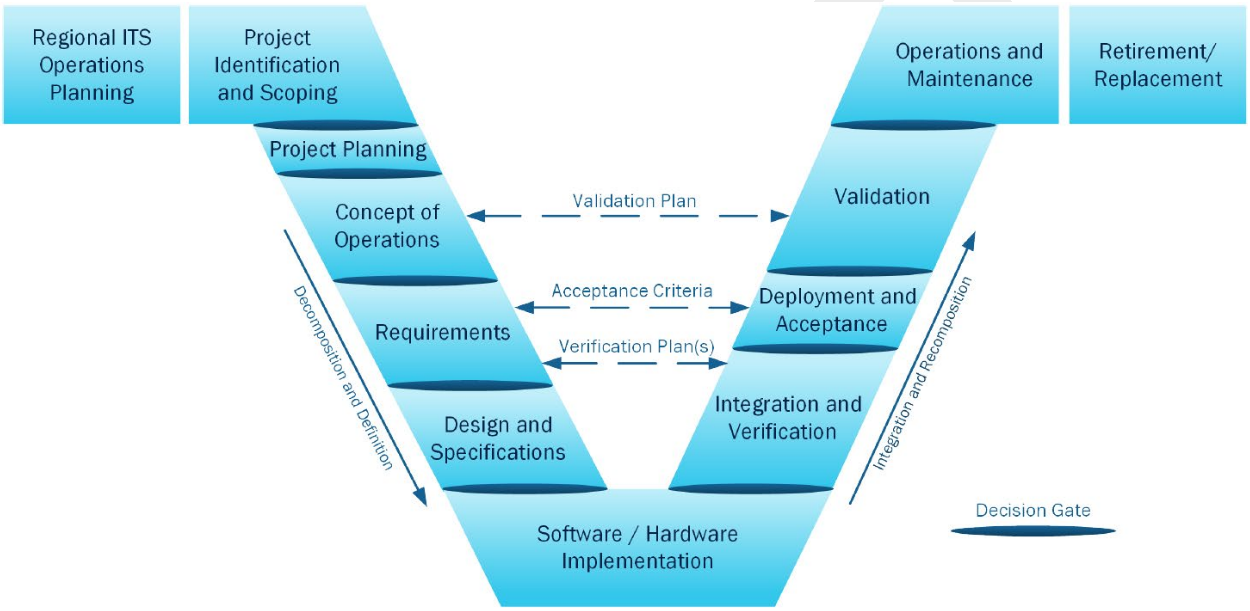

Figure B1 - Systems engineering "vee" diagram (Source: FHWA/Figure 10 of SE ITS document[5])

Once the system is defined, implementors will travel along the bottom part of the "vee" diagram, then up the right side, which consists of the following process stages:[6]

- Software and Hardware Implementation stage, when the hardware and software development activities occur, are monitored, and coordinated. Monitoring is accomplished by a preplanned series of reviews coordinated with the development team. These reviews provide early warning if requirements are deficient, or if they are not being fulfilled by the implementation.

- Integration and Verification stage, when the system is produced or manufactured. During this stage, the software and hardware components are individually verified and then integrated to produce higher level assemblies or subsystems. These subsystems are also individually verified before being integrated with other subsystems, until the complete system has been integrated and verified.

- Deployment and Acceptance stage, when the system is installed and operated by an IOO in its intended environment. Acceptance tests are performed either by the IOO, its representative(s), and/or the overall system vendor(s) to confirm that the system performs as intended in the operational environment before control is transferred. In this context, acceptance, and therefore conformance with CTI 4501, if specified correctly, is by the procuring IOO. System acceptance in terms of CTI 4501 conformance must also include SCMS compliance testing.

[5] Refer to https://ops.fhwa.dot.gov/seits/sections/section3/3_3_1.html.
[6] Systems Engineering for ITS

- Validation stage, when the operational system is confirmed to satisfy the user needs of the procuring IOO (or owner) and its stakeholders. From a deployment point of view, this stage is performed during a Burn-in period during which the system is under operational test with all its components (central system, field devices, and connecting communications infrastructure). The Burn-in periods used for the infrastructure central systems are typically between 30 and 90 days. The purpose of the Burn-in period is always two-fold:
  - Dealing with final system acceptance testing under operational conditions (i.e., as part of the verification tests, does the provided system still conform with the requirements while under longer-term operational use?). An IOO is reasonably expected to transfer the system to its own staff (and start the Operations and Maintenance stage of the project) after the vendor successfully demonstrated fulfillment of all requirements (this does NOT extend to any NON-SCOPED findings during the Burn-in period).
  - Determine (validate) whether the IOO specified the correct system and determine whether modifications (in scope or out of scope) are needed to satisfy user needs not thought about before.
- Operations and Maintenance stage, when the procuring IOO operates the system in its typical operational state. System maintenance is routinely performed and performance measures are monitored. As issues, suggested improvements, and technology refreshes are identified, they are documented, considered for addition to the system baseline, and incorporated. This documentation also includes any findings from the Burn-in period that were not in the originally scoped requirements.

An abbreviated version of the systems engineering process is used to evaluate and implement each change or modification. This occurs for each change or upgrade until the ITS system reaches its end-of-life.

B.1.3 Verification versus Validation

Verification and validation are two independent procedures. The INCOSE Systems Engineering Handbook explains the difference: "Verification ensures you built the system right (per the specifications). Validation ensures you built the right system."

ISO/IEC/IEEE 15288 defines the purpose of the validation process as:

> 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.

The INCOSE Systems Engineering Handbook defines the verification process as:

> Evidence is provided that the system, the system elements, and the work products in the life cycle meet the specified requirements.

Note where the Verification Plan and Validation Plan are found in the Systems Engineering "Vee" Diagram in Figure B1.

Section 8, Connected Intersection Testing, describes the purpose and contents of the verification plan to test for CTI 4501 conformance, along with some example content.

B.2 DEVELOPING A TEST FRAMEWORK

This section outlines guidance on the elements of a test framework in general, but with a focus on a test framework for a connected intersection. This section attempts to guide IOOs in organizing test processes, activities, and tasks in support of the (connected intersection) system life cycle, including during operations and maintenance. This section does not provide detailed guidance on testing procedures or on test planning activities such as testing tasks, personnel responsibilities, timeline, etc.; however, high-level examples are provided.

As noted above, testing should occur during every stage of a connected intersection's life cycle starting with the Software/Hardware Implementation stage; from when the individual components of a connected intersection are first produced (Software/Hardware Implementation); to when the connected intersection is accepted by the procuring agency (Deployment and Acceptance); until the connected intersection is operated and maintained (Operations and Maintenance); and all the steps in between.

This section:

- Presents an overall validation workflow.
- Summarizes the components of a connected intersection that need to be tested.
- Highlights the different types of requirements that need to be tested.
- Breaks down the testing process and highlights what functionality can be tested during each stage, including what requires revalidation after a CI system is changed.
- Provides references to relevant requirements and test specifications that can be used to create test procedures.

There are three dimensions of testing presented in this section. The three dimensions are:

- Component Under Test: The component of the connected intersection being tested;
- Types of Requirements Testing: The type of requirements being tested; and
- Testing Stages: The testing activities for each stage in the system life cycle and the goal of the testing activities.

B.2.1 Component under Test

The first testing dimension describes what is being tested – the component under test. The component could be a hardware device (e.g., a traffic signal controller or RSU); a communications interface (e.g., between the controller and RSU or between the RSU and OBU); a security certificate; a message (e.g., SPaT message, MAP message, RTCMcorrections message); or the overall system (i.e., the connected intersection).

Testing of each component reduces the risk of misinterpretation between agency and manufacturers of the component so that the CTI 4501 requirements are properly fulfilled. While early testing increases the upfront costs for the implementation, that testing cost is much lower than the costs associated with detecting and resolving and retesting any issue at a later deployment stage.

Figure B2 is similar to Figure 2, which is a graphical depiction of the physical architecture of a connected intersection, but includes the interfaces that are within the scope of the testing framework for a connected intersection.

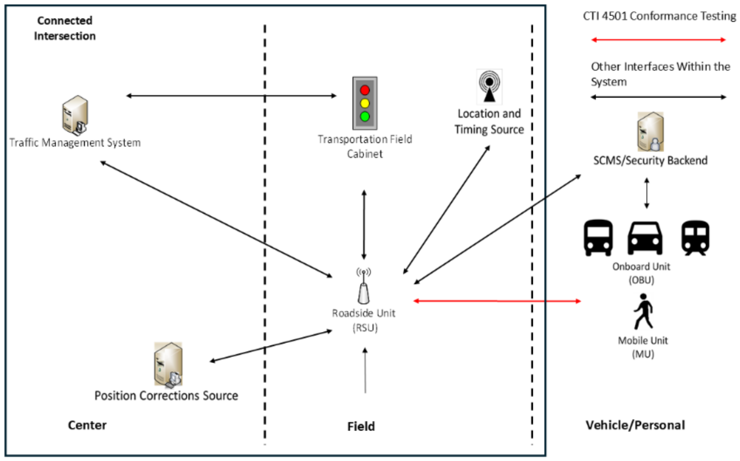

Figure B2 - Connected intersection components

The physical components of a connected intersection, repeated from CTI 4501, 5.3.1, are listed below, followed by any standards or specifications that may apply to that device. The standards or specifications listed may define requirements and/or test procedures for the device.

- 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. No current standard or specification.

- SCMS/Security Backend: A system that provides and manages security certificates to support trust within the CI system. No current standard or specification.

- Roadside Unit (RSU): A transportation field device that performs the data exchange between OBUs, MUs, and other infrastructure elements. Hardware, environmental, functional, and performance requirements are defined in CTI 4001. Complementary functional requirements can be found in NEMA TS 40010.

- Transportation Field Cabinet: A traffic cabinet containing devices and electronic systems that monitor and control traffic operations on a roadway. Includes the TSC that allows different conflicting movements to traverse the intersection in a safe, orderly manner. Physical, environmental, and electrical requirements are defined by NEMA TS 2 and ATC 5301. An IOO generally specifies either NEMA TS 2 or ATC 5301 for its agency.

- Location and Timing Data 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.

In addition to the physical components defined above, there are other physical components that comprise a connected intersection but are not represented in Figure 2. These include:

- TSC Infrastructure: The TSC infrastructure is a field device that controls traffic operations on a roadway, allowing different conflicting movements to travel across a roadway in a safe, orderly manner. The physical, environmental, and electrical requirements for a TSC are defined in NEMA TS 2 and/or ATC 5201. There are older TSC standards (e.g., NEMA TS 1, Model 170) that may be adopted by an agency, but those standards generally are unable to fulfill the performance requirements specified in CTI 4501. An IOO generally specifies one of these TSC standards for its agency.

- Connected Intersection Performance Monitoring System: The Connected Intersection Performance Monitoring System (CPMS) is a TMS that continuously monitors the movement of connected vehicles at a signalized intersection and compares the movements with the contents of the MAP message.

Another component of a connected intersection that requires testing is the communications interface. Communications interface testing consists of testing the interface to verify that the interface fulfills the interface requirements. The communications interfaces are depicted in Figure B2 by the arrows between the physical components.

- RSU – OBU/MU: Depicted by a red solid arrow, this communications interface allows V2X messages to be exchanged between the connected intersection (via the RSU) to OBUs and MUs. This communications interface is the focus of CTI 4501, which defines the minimum requirements for information to be exchanged across this communications interface in support of RLVW applications. Standards referenced by CTI 4501 for this communications interface include SAE J2735 (such as the SPaT, MAP, RTCMcorrections, and BSM messages), SAE J3161, and 3GPP TS 23.285. Other standards may define minimum requirements across this interface to support other V2X applications. This interface is the focus of CTI 4501 conformance testing (see Section 8).

- RSU – SCMS: Depicted by a black solid arrow indicating it is a required supporting interface, this communications interface allows for the exchange of certificates and CRLs between an SCMS provider and the RSU. Standards that define this communication interface include IEEE Std 1609.2 and IEEE Std 1609.2.1.

- Traffic Management System – RSU: This communications interface allows a TMS to configure, monitor, and control RSUs, and forward or receive V2X messages that are broadcasted or received by the RSU. Standards that define this interface include NTCIP 1218. V2X messages may include MAP messages.

- Location and Timing Source – RSU: This communications interface provides position and time from a GNSS receiver. Standards that define this interface include SAE J3258.

- TSC Infrastructure – RSU: This communications interface allows a traffic signal controller to provide signal phase and timing information to the RSU so the RSU can broadcast SAE J2735 SPaT messages. Standards and specifications that define the signal phase and timing information include NTCIP 1202, TSCBM, and SAE J2735. Note: TSCBM is not recommended for new installations.

- Position Corrections Source – RSU: This communications interface provides RTCM correction messages. These messages will be used to generate SAE J2735 RTCMcorrections messages. This interface may be implemented by NTRIP 1.0 and 2.0.

B.2.2 Types of Requirements Testing

The type of requirements testing is dependent on the types of requirements defined for a connected intersection. Examples of types of CI requirements, and thus types of testing include functional, performance, communications interface, electrical, mechanical, environmental, and security.

Section B.2.1 lists some of the standards that define requirements for several of the components that comprise a connected intersection. Each standard may define different types of requirements for that component. For example, CTI 4001 contains environmental, electrical, mechanical, functional, performance, and security requirements for the RSU, while NEMA TS 2 defines electrical, environmental, and functional requirements for the TSC and the traffic cabinet. The CTI 4501 family of documents define the requirements for a connected intersection.

Table B1 summarizes some of the types of requirements defined within the standards mentioned in B.2.1.

Table B1 - Type of requirements by standard

Standard	Types of Requirements						
	Functional	Performance	Environmental	Electrical	Mechanical	Security	Communications
3GPP TS 23.285							✓
ATC 5201	✓		✓	✓	✓		
ATC 5301			✓	✓	✓		
CTI 4501 Family	✓	✓					✓
CTI 4001	✓	✓	✓	✓	✓	✓	
IEEE Std 1609.2						✓	
IEEE Std 1609.2.1						✓	
IEEE Std 1609.2.2						✓	
NEMA TS 2	✓	✓	✓	✓	✓		
NEMA TS 40010	✓	✓	✓				✓
NTCIP 1202		✓					✓
NTCIP 1218		✓					✓
SAE J2735							✓
SAE J3161							✓

In addition to the requirements defined by the standards referenced, an agency may have its own specification requirements for the hardware, software applications, and for security for the field devices deployed by the IOO.

B.2.3 Testing Stages

Because of its safety critical nature, from when a component of a connected intersection is first produced, until the system is retired, testing is required to **continuously** verify and validate that the connected intersection operates as intended. This continuous testing process is to ensure system reliability, performance, safety, and compliance with specifications to satisfy the selected user needs.

The purpose of testing varies from stage to stage through the life of a complex system such as a connected intersection. For example, the purpose of a connected intersection revolves around the exchange of information between the infrastructure and an OBU/MU. The process of message creation and transmission broadcasted by the connected intersection involves multiple CI components and interfaces, as depicted in Figure B2.

The Systems Engineering for ITS (and the vee diagram) document defines the following stages of a system:

- Software and Hardware Implementation
- Integration and Verification
    - Component Testing
    - Integration Testing
    - Deployment and Acceptance
- Integration Field Testing
    - System Testing
- Validation
    - Burn-in Testing
- Operations and Maintenance
    - Ongoing System monitoring
    - System maintenance

In summary, the approach to testing the connected intersection involves testing each individual component first, followed by testing the integrated system as a whole. Various components will be tested separately and then put together into a system and tested together during the Integration and Verification stage. The Deployment and Acceptance stage includes testing various capabilities of the connected intersection system by an IOO before and after system deployment at an intersection. During the Validation stage, the goal is to prove system operation, performance, and stability running under a variety of operational scenarios and conditions. The Operations and Maintenance stage defines the testing while the connected intersection is in operation, including testing after a (component) failure or any (software or hardware) updates to a CI component.

B.2.3.1 Software and Hardware Implementation

During the Software and Hardware Implementation stage, various components of a connected intersection system are procured. Some IOO specifications require a vendor to provide comprehensive testing reports that confirm that the components being procured, such as the TSC or traffic cabinet, fulfill the requirements of the specification. Some components, such as an RSU, can be tested by independent test laboratories as part of an independent certification program.

B.2.3.2 Integration and Verification

The Integration and Verification stage consists of the performance of tests in the following sequence:

- Component Testing: Generally performed in a laboratory environment, component testing focuses on verifying the functionality and performance of individual parts or modules within the connected intersection. The primary goal is to ensure that each component operates as expected in isolation before it's integrated with other components of the connected intersection. These components could range from hardware elements (such as RSU or TSC) to software elements (like functionality supporting AGP). SCMS Security Policy requires certified V2X devices to issue production certificates.

- Integration Testing: Typically performed in a "controlled" laboratory test environment, integration testing evaluates how different components work together to fulfill the requirements of a connected intersection. Integration testing is crucial for identifying issues related to data exchange, interoperability, and communication between various subsystems or modules. For instance, integration testing may check if the information contained in transmitted SPaT messages is synchronized with the signal phase and timing managed by the TSC itself.

Note that integration testing is an iterative process. From the FHWA Systems Engineering for ITS document:

> Integration and verification is an iterative process in which the software and hardware components that make up the system are progressively combined and verified against the requirements as shown in Figure 20 [Figure B3 in CTI 4501/4]. This process continues until the entire system is integrated and verified against all of its requirements.

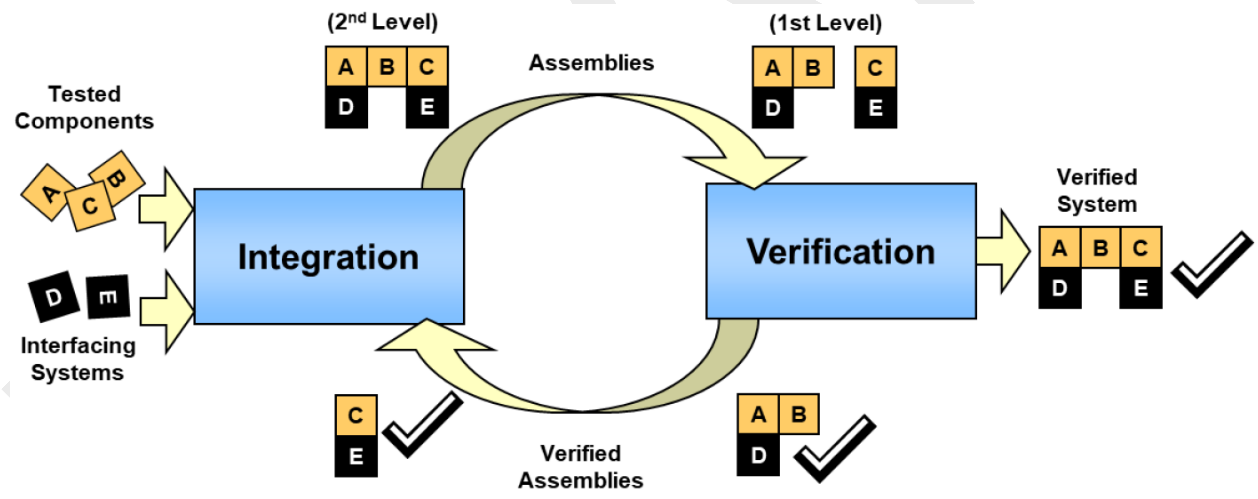

Figure B3 - Verification process

B.2.3.3 Deployment and Acceptance

During deployment and before/during acceptance testing, the issue of interchangeability between products from different vendors (sometimes even between models from the same vendor) that are required to fulfill the same set of requirements comes up. Theoretically, devices fulfilling the same requirements should be interchangeable, but that statement must be followed by testing. When designing a test plan that is to address interoperability, one needs to consider that the standardized CTI 4501-defined requirements do not require how a device works internally but instead largely address inputs and outputs requirements. Within a test plan, the test cases need to focus on those – with the understanding that values determined through model-specific algorithms internal to the device under test might produce slightly different values. As CTI 4501 is focused on RLVW applications, an IOO responsible for deploying connected devices needs to consider that any device claiming conformance to CTI 4501 and also claiming interoperability with existing devices conformant to CTI 4501 can only make this claim pertaining to the RLVW application and the underlying data exchange methodologies.

The Deployment and Acceptance stage consists of the performance of tests in the following sequence:

- Integration Testing – Field: Field integration testing evaluates how different components of a connected intersection work together when the components are installed in their intended operational environment. This type of testing is crucial for identifying issues related to data exchange, interoperability, and communication among the various components. Stand-alone testing should be performed prior to field integration testing. Stand-alone tests are performed to check that components are not damaged during transport to the deployment site.

- System Testing: System testing is conducted after the connected intersection is installed at the target location. System testing assesses the complete and fully integrated connected intersection's compliance with the specifications, including the requirements in CTI 4501. System testing may encompass evaluating both functional aspects (e.g., validates that the connected intersection transmits compliant SPaT, MAP, and RTCM messages) and non-functional aspects (e.g., reliability, security, performance).

  System testing must include end-to-end (E2E) testing which examines CI data exchanges with other systems such as the provider of SCMS certificates, sources of RTCMcorrections messages, and communication with the CPMS. System testing could also include drive tests near the target intersection to validate RSU communication range and spatial accuracy of MAP messages.

  In addition to all CI components (hardware and software) deployed at an intersection, system testing should also consider and validate certain configuration items in the context of the deployment site listed below:

  - Site specific RSU configuration parameters
  - TSC timing plans/databases compatibility with RSU configuration
  - TSC application processor software and configuration
  - Security settings
  - MAP files
  - Networking parameters used on routers and firewalls managing network flow in the traffic cabinet
  - Connection to CPMS
  - Connection to SCMS

  Successful completion of Systems Testing is usually a requirement for systems acceptance, as a contractual milestone for the owning agency to formally pre-accept the system to go into the Burn-in Period, which is part of a full system acceptance. Formal systems acceptance using the approved test plan and its test cases and test procedures is often a contractual trigger for payment, and definitely the milestone for the start of operational verification (and validation) activities (Burn-in Testing) and the start of the warranty or service period.

  Successful completion of Systems Testing may also be a prerequisite for operational certificates from a SCMS provider.

B.2.3.4 Validation

The Validation stage consists of testing and monitoring during a defined duration period, the Burn-in period. This form of testing is a time-bound operation of an installed CI system continuously operating for an extended period (e.g., a few weeks) with CPMS system monitoring in place. The purpose is to identify misconfigurations, early failures, and ensure reliability before final acceptance of all system components and transition into the Normal mode. During the Burn-in Period, certain tests performed previously/defined in the test plan might be repeated or the IOO might decide to just operate the system to ensure everything works as intended.

For example, for new intersections, Burn-in testing with system monitoring over a period of at least 4 weeks may confirm RSU operation under different traffic conditions, allow RSUs to retrieve two certificate changes from SCMS, and provide CPMS with ample time to collect data and report on any exceptions.

The Burn-in Period also offers the IOO/system owner an opportunity to determine whether all requirements were actually stated correctly or whether requirements were forgotten or have newly been determined. The IOO/system owner would capture these types of new user needs and/or new or modified requirements for future developments and/or enhancements recognizing that these are not part of the current system's scope. To avoid mixing current contract acceptance and possible enhancements or new requirements, it is recommended to first perform the Burn-in Period to verify current system requirements, and after successful completion of the Burn-in Period, start with the validation checking.

For example, certain capabilities generally possible with RSUs are determined to be of high interest to the IOO, or certain means to display results are desired to be shown differently.

B.2.3.5 Operations and Maintenance

At this stage, the CI system continues its operation and an intersection is recognized as a fully verified and accepted connected intersection. The CPMS monitors the connected intersection with the purpose of monitoring, identifying, and reporting on system exceptions and controlling the CI system running mode. CPMS reports may also be used to demonstrate a connected intersection's continued compliance with the operating requirements.

During this stage, verification activities will continue to ensure that the connected intersection operates under its target intersection environment such as when it is connected to the field network, the SCMS provider, and CPMS; and that the SPaT and MAP message contents accurately reflect operations at the intersection.

A connected intersection is anticipated to change over time. Component replacements due to malfunctions or obsolescence, firmware/software updates, and configuration alterations may require at least a partial reverification before normal operations can resume. Other changes may arise from road maintenance or repairs, which could impact TSC operation or necessitate updates to MAP messages. On top of that, critical issues may also cause the connected intersection to switch into a Maintenance mode.

In general, the return path into Normal mode after any modifications should include some reverification. If the issue has resolved itself, the reverification may be focused on the root cause of the issue. Afterwards, the connected intersection should be returned to Normal mode.

If changes to the connected intersection are minor and covered within the scope of the original system verification, at a minimum, the repeat of a Burn-in testing is recommended to monitor and confirm system operation. If changes are greater in scope, then verification may involve repeat of some of preceding testing steps – system, integration, and even some component testing. Examples of changes that should require verification activities:

- CI Configuration Changes: software, firmware, hardware changes
- Changes in Standards supported: SAE J2735 version
- Message element table: Mandatory Elements, Optionals made Mandatory, Conditional
- Controller Parameters: e.g., Timing plans

B.2.4 Example Testing by Component(s)

This section offers several operational scenarios and provides guidance on the scale and scope of revalidation after changes. An IOO is expected to take on the responsibility of defining more specific guidelines and conditions which will determine the extent of the reverification and ensure consistency with the requirements of the SCMS provider.

The components for which examples are provided are:

- CTI Conformance Testing by Stage
- Connected Intersection Testing
- RSUs
- Traffic Signal Controllers
- Traffic Cabinets
- Security

B.2.4.1 Planned Activities by Stage

Generally, CTI 4501 conformance testing activities are performed at least twice during the life cycle of a connected intersection. The first time is as part of Integration Testing in a controlled test environment, after the components of the connected intersection are combined. CTI 4501 conformance testing activities might be performed only once in the controlled test environment.

The second time is as part of Integration Field Testing after the connected intersection components are installed in its intended location, and system integration activities are completed. It is recommended that CTI 4501 conformance testing be performed for every installed connected intersection, to confirm that the hardware and software is properly configured and the connected intersection operates as intended. CTI 4501 conformance testing should be completed and accepted as a requirement for systems acceptance and prior to the start of the validation activities (Burn-in Testing).

A subset (or the complete set) of the conformance testing may be repeated during any other testing stages, as defined by the implementation agency's test policies and procedures. If CTI 4501 conformance testing is to be performed during other stages of the connected intersection's life cycle, the test environment for each stage may be described in the verification plan. The verification procedures for a specific test case may also be different for each stage.

B.2.4.1.1 CTI 4501 Conformance Testing by Stage - SPaT Messages

Refer to CTI 4501/1 Table 9 for an example of when a subset of CTI 4501 conformance testing for SPaT messages may be performed or repeated during the different stages of a connected intersection's life cycle.

B.2.4.1.2 CTI 4501 Conformance Testing by Stage - MAP Messages

Refer to CTI 4501/2 Table 7 for an example of when a subset of CTI 4501 conformance testing for MAP messages may be performed or repeated during the different stages of a connected intersection's life cycle.

B.2.4.1.3 CTI 4501 Conformance Testing by Stage - RTCMcorrections Messages

Table B2 represents an example of when a subset of CTI 4501 conformance testing for RTCMcorrections messages may be performed or repeated during the different stages of a connected intersection's life cycle.

Table B2 - Verification by stage - RTCMcorrections message

Stage	Test Scope
Certification	Message elements are verified as part of Device-level certification
Component Testing	Verification of message elements and testing device interoperability
Integration Testing	Perform all test cases for all mandatory and selected requirements
Integration Testing – Field	Minimally perform the test cases for a subset of mandatory and selected requirements
System Testing	Perhaps perform the test cases for a subset of mandatory and selected requirements
Burn-in Testing	Perhaps perform the test cases for a subset of mandatory and selected requirements
Operations and Maintenance	Perform a subset of SAE J3258 after changes to firmware or hardware

B.2.4.1.4 CTI 4501 Conformance Testing by Stage - BSM Messages

Table B3 represents an example of when a subset of CTI 4501 conformance testing for BSM messages may be performed or repeated during the different stages of a connected intersection's life cycle.

Table B3 - Verification by stage - BSM message

Stage	Test Scope
Certification	Message elements are verified as part of Device-level certification
Component Testing	Verification of message elements and testing device interoperability
Integration Testing	Perform all test cases for all mandatory and selected requirements
Integration Testing – Field	Minimally perform the test cases for a subset of mandatory and selected requirements
System Testing	Perhaps perform the test cases for a subset of mandatory and selected requirements
Burn-in Testing	Perhaps perform the test cases for a subset of mandatory and selected requirements
Operations and Maintenance	To be determined

B.2.4.1.5 CTI 4501 Conformance Testing by Stage - Security

Table B4 represents an example of when a subset of CTI 4501 conformance testing for security may be performed or repeated during the different stages of a connected intersection's life cycle.

Table B4 - Verification by stage - Security

Stage	Test Scope
Certification	Device Certification for security from a certification body
Component Testing	Not Applicable
Integration Testing	Perform all test cases for all mandatory and selected requirements
Integration Testing – Field	Minimally perform the test cases for a subset of mandatory and selected requirements
System Testing	Perhaps perform the test cases for a subset of mandatory and selected requirements
Burn-in Testing	Perhaps perform the test cases for a subset of mandatory and selected requirements
Operations and Maintenance	Perform a subset of SAE J3258 after changes to firmware or hardware

B.2.4.2 Connected Intersection Testing

This section presents examples of the types and stages of testing that may be performed for a connected intersection (CI) as a whole.

B.2.4.2.1 CI - Integration Testing

The focus of Connected Intersection Testing is the requirements for the connected intersection as a whole – not the individual components that comprise the connected intersection. As such, any testing of the connected intersection begins with integration testing.

Integration testing in the laboratory setting can cover a large portion of the expected verification between RSUs and the TSC Infrastructure. Table B5 lists functionality expected to be tested during this phase and lists relevant specifications.

Table B5 - Verification scope for the system integration testing

#	Capabilities	Focus Areas	Relevant Specification
1	CI message conformance	a. Conformance of SPaT broadcasts	CTI 4501
		b. Conformance of MAP broadcasts	CTI 4501
		c. Conformance of RTCM broadcasts	SAE J3258
		d. Message content, structure, bounds checking for the above messages	CTI 4501
2	CI security capabilities	a. Message signing & verification, CRL, misbehavior reporting	IEEE Std 1609.2
		b. Interface to SCMS	IEEE Std 1609.2.1
		c. Security penetration	Agency provided
3	CI system anomaly testing	a. CTI operation and reliability in typical configurations – TSP, EVP, free running, coordinated, transition, etc.	Agency provided
		b. CI recovery under "imperfect" power conditions and outages	Agency provided
		c. CI recovery after network/communication interruptions	Agency provided
		d. CI recovery after component change/outage	Agency provided
		e. Detection of invalid signals, recovery from CMU trigger	Agency provided

"Agency provided" refers to the documentation that are internal to the agency and not a published industry standard. However, the corresponding testing focus still merits development of a testing approach that is expected to be undertaken by individual IOOs, at least initially.

CTI 4501 defines:

- Mandatory data elements to be included in a SPaT and MAP message to support a RLVW application
- Message structure and data format as outlined in SAE J2735
- Data values within the range specified in SAE J2735

CTI 4502, SAE J3238/1, and SAE J3238/2 provide examples of how to test for the conformance of SPaT and MAP broadcasts.

CTI 4502 describes the test tools/procedures for conformance during Phase 1 of the Connected Intersections project. The conformance testing focused on verifying that the SPaT and MAP message broadcasted from 14 volunteer validation sites fulfilled the functional requirements in CTI 4501. More specifically, the tools and procedures verified that the mandatory data elements are in the broadcasted SPaT and MAP messages, and that the data elements in the messages conformed to the structure and value range specified in SAE J2735. However, Phase 1 validation testing did not completely examine if the values in the broadcasted SPaT and MAP messages are correct.

For example, if the SPaT messages indicated that a through movement at the intersection was green, the test tool and procedures did not confirm that the through movement at that intersection was actually green.

SAE J3238/1 and SAE J3238/2 provide additional examples of how to extend conformance testing to consider performance requirements. Both SAE documents assume that the functional over-the-air message conformance is verified and tests the correctness of the message data against ground truth (e.g., are the current movement states reported in the SPaT message accurate) and the performance requirements (e.g., are the node positions reported in the MAP message within 20 centimeters of the actual node positions).

A subset of the integration testing in the laboratory setting may also be repeated when all the components of the connected intersection have been performed in the field. The purpose of integration testing at its operational location is to verify that the data exchange, interoperability, and communications among the various components.

B.2.4.2.2 CI - System Testing

Once integration testing is completed, system testing focuses on certain areas that may be altered after the connected intersection is installed at an intersection. System testing may repeat some of the integration tests previously performed; however, its focus will be to ensure that the connected intersection is properly set up and configured for the target intersection. Examples of the targeted capabilities, focus areas and relevant specifications are listed in Table B6.

Table B6 - End-to-end intersection testing target verification scope

#	Capabilities	Focus Areas	Relevant Specification
1	Radio coverage	a. Confirm RSU signal reachability in all directions of travel	CTI 4501
2	CI message transmissions	a. SPaT mandatory fields, accuracy & latency	CTI 4501
		b. MAP mandatory fields	CTI 4501
		c. MAP node positional accuracy to the intersection	CTI 4501
		d. RTCM required message types	SAE J3258
3	CI message mutual consistency	a. SPaT and MAP mutual consistency	CTI 4501
		b. SPaT and MAP consistency to the physical intersection layout	CTI 4501
4	CI security	a. Use of certificates to sign and verify messages, CRLs, misbehavior reports	IEEE Std 1609.2
		b. Accessing SCMS to download RSU certificates and upload misbehavior reports	IEEE Std 1609.2.1

B.2.4.2.3 CI - Burn-In Testing

During Burn-in testing, the connected intersection operates in Normal mode, except particular attention will be given to anomalies and exceptions that may be detected in the connected intersection by the CPMS or other monitoring system. Typical duration of the system Burn-in testing would be established by an IOO based on its experience and system complexity, but it is expected to last at least 4 weeks assuming no critical issues are discovered.

Table B7 provides examples of typical failures that have been observed during previous CI deployments and may be useful for monitoring during the system Burn-in period.

Table B7 - Listing of typical CI anomalies and detection methods

#	CI Anomalies	Detection & Validation
1	MAP misalignment with ground truth, e.g., missing lanes due to road construction	CPMS is expected to detect such misalignments with sufficient penetration of connected vehicles.
2	Misalignment between SPaT/MAP due to controller reconfiguration, map changes, etc.	CPMS is expected to detect such misalignment by comparing contents and mutual consistency of SPaT and MAP messages.
3	RSUs off-line, missing messages due to network outages or hardware issues.	CPMS can detect RSU outage by monitoring network access to RSU and monitoring its operating parameters.
4	Lack of message transmissions due to security certificate issues.	CPMS can detect loss of message transmissions by monitoring RSU operating parameters. Checking for RSU certificates may be handled by other methods e.g. using SCMS provider dashboard, etc.

B.2.4.2.4 CI - Operations and Maintenance

Over its operational life cycle, the connected intersection will likely experience failures due to external events (e.g., power failures, communications interruptions), hardware may be upgraded, and software will be updated. After each of these events, verification activities are recommended before the connected intersection is placed back into Normal mode. Table B8 presents some verification activities to perform after specific changes (events) during the operational life cycle of a connected intersection.

Table B8 - Reverification caused by changes in other system components

#	Domain of Changes Description of Change	Reverification	Notify SCMS Provider
1	Software updates to CPMS	Integration tests focused on the area of change or selected based on the need to manage the risk of change. Followed by Burn-in testing.	
2	Updates in the infrastructure providing GNSS corrections	Partial Integration testing focused on RTCM provider interface, followed by the System testing and Burn-in testing.	
3	MAP message updates after major intersection configuration changes (lanes, phase assignments)	Validate MAP message accuracy and conformance.	

B.2.4.3 RSUs

This section presents examples of the types and stages of testing that may be performed for an RSU.

B.2.4.3.1 RSU - Software and Hardware Implementation

Independent certification testing is required as a prerequisite step prior to IOO performing Component Testing and Integration Testing and allows for production security certificates. Table B9 includes a minimum scope of RSU certification testing modeled after the OmniAir RSU certification. RSU devices that pass these tests and fulfill certain other certification criteria are recorded as "Certified RSUs" in the OmniAir certification registry, which is accessible to IOOs. Table B9 is an example of certification process (others may do something similar).

Table B9 - RSU certification testing

#	Capabilities	Focus Areas	Relevant Specification
1	RSU environmental verification	a. Temperature, Humidity, Precipitation, etc. b. Shock & Vibration, Wind resistance c. Mounting d. Grounding e. Resistance to ESD & EMI via antenna and PoE f. Power Protection & Filtering g. Power (PoE)	CTI 4001 " " " " " IEEE Std 802.3 (Note: Specifically, IEEE Std 802.af or IEEE Std 802.3at)
2	RSU conformance in wireless interfaces	a. Spectral mask, out-of-band emissions, etc. b. Radio and media access c. WAVE Networking Services d. V2X Message Set Dictionary e. OBU System Requirements for LTE-V2X Safety	FCC 3GPP IEEE Std 1609 SAE J2735 SAE J2945
3	RSU SPaT messaging capabilities	a. TSC capabilities to create SPaT b. MAP transmissions c. RTCM broadcasts	NTCIP 1202, SAE J3238/1 SAE J3238/2, CTI 4502 SAE J3258
4	RSU MIB interface conformance	a. MIB object definition for RSUs	NTCIP 1218
5	RSU security capabilities	a. Message signing & verification, misbehavior reporting b. Interface to SCMS	IEEE Std 1609.2 IEEE Std 1609.2.1

Devices that successfully pass the certification testing programs provide higher assurance to be compliant to industry-adopted test specification and carry the additional benefit of being tested for interoperability and interchangeability with other certified devices. Typically, certification testing is carried out by independent third-party laboratories before RSUs are procured. Therefore, any changes required for the RSUs to acquire certification status are already implemented prior to IOO procurement. These tests are to be performed to fulfill the requirements in CTI 4001 and NEMA TS 40010.

Gathering test results and reports from the vendor and certification test laboratory is also important. This documentation is incorporated into a verification report that will be submitted to the SCMS Provider and become part of the acceptance documentation for the connected intersection.

B.2.4.3.2 RSU - Operations and Maintenance

During the Operations and Maintenance Stage, an RSU may be subject to firmware/software updates, and configuration alterations may require at least a partial reverification before normal operations can resume. Table B10 lists types of changes that may occur and what testing may be required before an RSU is placed back into full service. The reverification approach may vary by IOO.

Table B10 - Reverification caused by changes with RSUs

#	Description of Change	Reverification Approach	Notify SCMS Provider
1	RSU swap-out in the field for a different device within the same domain (supporting the same CV end application) without changing device model or firmware version.	No revalidation.	Yes. New RSU requires new certificates provisioning.
2	RSU firmware update. No change to device hardware.	Partial system integration focused on RSU functionality and TSC interface followed by Burn-in testing.	No.
3	RSU replacement with a different model or vendor.	Integration testing followed by system testing and Burn-in testing.	Yes. New RSU requires new certificates provisioning.

B.2.4.4 Traffic Signal Controllers (TSC)

This section presents examples of the types and stages of testing that may be performed for a TSC infrastructure.

B.2.4.4.1 TSC - Component Testing

During component testing, the TSC or the TSC Infrastructure is verified to conform with the appropriate TSC standards and the appropriate TSC infrastructure requirements defined in CTI 4501. Table B11 lists some of the capabilities (and requirements) that may be tested as part of component testing.

Table B11 - TSC infrastructure component testing

#	Capabilities	Focus Areas	Relevant Specification
1	TSC capabilities to generate SPaT	a. Verification of TSC generated SPaT (if applicable)	CTI 4501, NTCIP 1202, SAE J3238/1
		b. CI latency measurements (SPaT vs cabinet serial bus)	NTCIP 1202, SAE J3238/1
		c. SPaT content, structure, bounds checking	CTI 4501
		d. Validation of SPaT correctness and reliability under various operational transitions and scenarios	CTI 4501
2	TSC MIB conformance	a. Conformance to SPaT MIBs b. Conformance to other vendor specific MIBs required for system monitoring	NTCIP 1202. Alternatively, agency provided test specs.
3	TSC Infrastructure anomaly testing	f. TSC Infrastructure operation and reliability in typical configurations – TSP, EVP, free running, coordinated, transition, etc. g. TSC Infrastructure recovery under “imperfect” power conditions and outages h. TSC Infrastructure recovery after network/communication interruptions i. TSC Infrastructure recovery after component change/outage j. TSC Infrastructure detection of invalid signals, recovery from CMU trigger	Agency provided " " " "

B.2.4.4.2 TSC - Operations and Maintenance

During the Operations and Maintenance Stage, the TSC Infrastructure may be replaced, subject to firmware/software updates, or configuration alterations may require at least a partial reverification before normal operations can resume. Table B12 lists types of changes that may occur and what testing may be required before the TSC Infrastructure is placed back into full service. The reverification approach may vary by IOO.

Table B12 - Reverification caused by changes with TSC

#	Description of Change	Reverification Approach	Notify SCMS Provider
1	TSC swap-out for a different device within the same domain (supporting the same CV end application) without changing device model or firmware version.	No reverification.	Yes, if the TSC generates full signed SPaT messages.
2	TSC firmware update No change to device hardware.	Partial system integration focused on RSU functionality and TSC interface followed by Burn-in testing.	Not necessary.
3	TSC replacement with a different TSC model or vendor.	Integration testing followed by the System testing and Burn-in testing.	Yes, if the TSC generates full signed SPaT messages.
4	TSC configuration updates in TSC configuration, timing plans, etc.	Partial system testing and Burn-in testing.	No.

B.2.4.5 Traffic Cabinets

This section presents examples of the types and stages of testing that may be performed for a TSC infrastructure.

B.2.4.5.1 Traffic Cabinet - Operations and Maintenance

During the Operations and Maintenance Stage, the components within a traffic cabinet may be replaced, subject to firmware/software updates, or configuration alterations may require at least a partial reverification before normal operations can resume. Table B13 lists types of changes that may occur and what testing may be required before the connected intersection is placed back into full service. The reverification approach may vary by IOO.

Table B13 - Reverification caused by changes in the traffic cabinet

#	Description of Change	Reverification Approach	Notify SCMS Provider
1	TSC Infrastructure or the ECLA hardware or software update	Partial Integration Testing focused on the TSC Infrastructure or ECLA; and interfaces to the TSC Infrastructure, ECLA and RSU followed by the System Testing and Burn-in Testing.	Yes, if TSC Infrastructure generates fully signed CV messages.
2	Any other cabinet devices Changes in load switches, power supplies, network/communication gear, SIU/CMU	Cabinet reliability testing performed by IOO.	No.

B.2.5 Security

This section describes an overall approach to security. It describes a security verification approach used that is consistent with the guidance presented in CTI 4501/3 and other standards (e.g., NTCIP or SAE). The approach includes Security Documents (SD) in CTI 4501/3 that should be completed as part of the security evaluation. This section also highlights acceptance criteria and captured reporting data from the security testing that can be used by the IOOs as part of an annual overall security audit. Recall that CTI 4501 focuses on the interface between connected intersection and OBUs/MUs, as depicted in Figure B2.

Security verification for a connected intersection is focused on overall system security, so message and communication interface security are expected to be handled as part of component and system integration testing, although some associated tests may be repeated as part of the final acceptance test and during the Burn-in period.

A connected intersection has exposed interfaces that need to be protected and therefore tested to ensure protection. Figure B2 depicts some of the interfaces within the connected intersection, and the interfaces to and from external entities. These interfaces are summarized as follows:

1. Connected Intersection to/from OBUs and MUs: The communications type across this interface is broadcast, where every receiving entity can receive data and decide whether to ignore or react to the received data. Data received but not applicable to the receiver is discarded without action or storing the data. A valid security certificate (defined by IEEE Std 1609.2) is a determination whether the sender of the data is a trusted entity. SAE J3287 describes whether the entities might be misbehaving (e.g., sending the wrong data or processing faulty data).

2. Connected Intersection to/from a Center: A TMS within a Center is typically a central software package that manages field devices and monitors its vitals; and can perform other diverse functions operated within a center. A CPMFS is an example of a TMS. The interfaces between a Center and a connected intersection are often a wireline connection via internet protocols (IP). NTCIP 1201, NTCIP 1202, and NTCIP 1218 cover the wireline interfaces from a data element point of view, while the underlying communications protocols are covered by other NTCIP standards such as NTCIP 2103, NTCIP 2202, and NTCIP 2301. These NTCIP standards may reference other security standards (e.g., DTLS 1.3) to protect these interfaces.

3. Interfaces among the Field Devices within the Connected Intersection: Field devices within the connected intersection include the RSU, a TSC, the traffic cabinet, and date/time source. The interface is generally a physical cable, but could be wireless. There are standards and specifications that may specify physical security for each field device, such as NEMA TS 2 for a TSC, or CTI 4001 for an RSU. Some communications standards, such as NTCIP 1202 and NTCIP 1218, for exchanging data among the field devices, may also reference security standards to protect these interfaces.

The security validation process for a connected intersection must consider the overall system security including the interfaces described above and the functional capabilities of the connected intersection, including those functions to support applications such as the RLVW application. The overall testing therefore includes both device-specific testing and interface testing.

A security validation process may include, but is not limited to, device certification from a certification body, performing verification tests, using a tool or a system to continuously collect data for verification, providing reports to a SCMS provider, receiving certificates from an SCMS provider, performing physical inspections on a periodic basis, and performance monitoring by a CPMS.

SCMS Manager Intersection Validation Policy establishes the requirements and procedures for validating connected intersections and issuing digital certificates. The document describes roles and responsibilities of different entities involved with issuing certificates, a validation process, and requirements for the end entity before issuing certificates. The validation process defined in the document details the initial verification (Section 5.1 - Validation Process) and certificate issuance process (Section 6.1 - Certificate Management). Note that this document defines additional requirements beyond the requirements in the CTI 4501 documents. For example, Section 5.2 has requirements for "continuous monitoring," which requires a tool that monitors the RSU continuously and provides weekly reports to be sent to SCMS provider.

CTI 4501 also requires that an implementation include a CPMS to continuously monitor and evaluate a connected intersection to determine if the system fulfills the performance requirements, including the connected intersection notifying the CPMS if it is in a degraded state or incorrect information is sent (refer to CTI 4501, 6.3.5).

Figure B4 represents an example of the report flow that an SCMS provider may require from an IOO through the connected intersection's life cycle for validating the connected intersection and issuing digital certificates. Refer to SCMS Manager's CI Test Results Report Format for a more detailed explanation about the report flow.

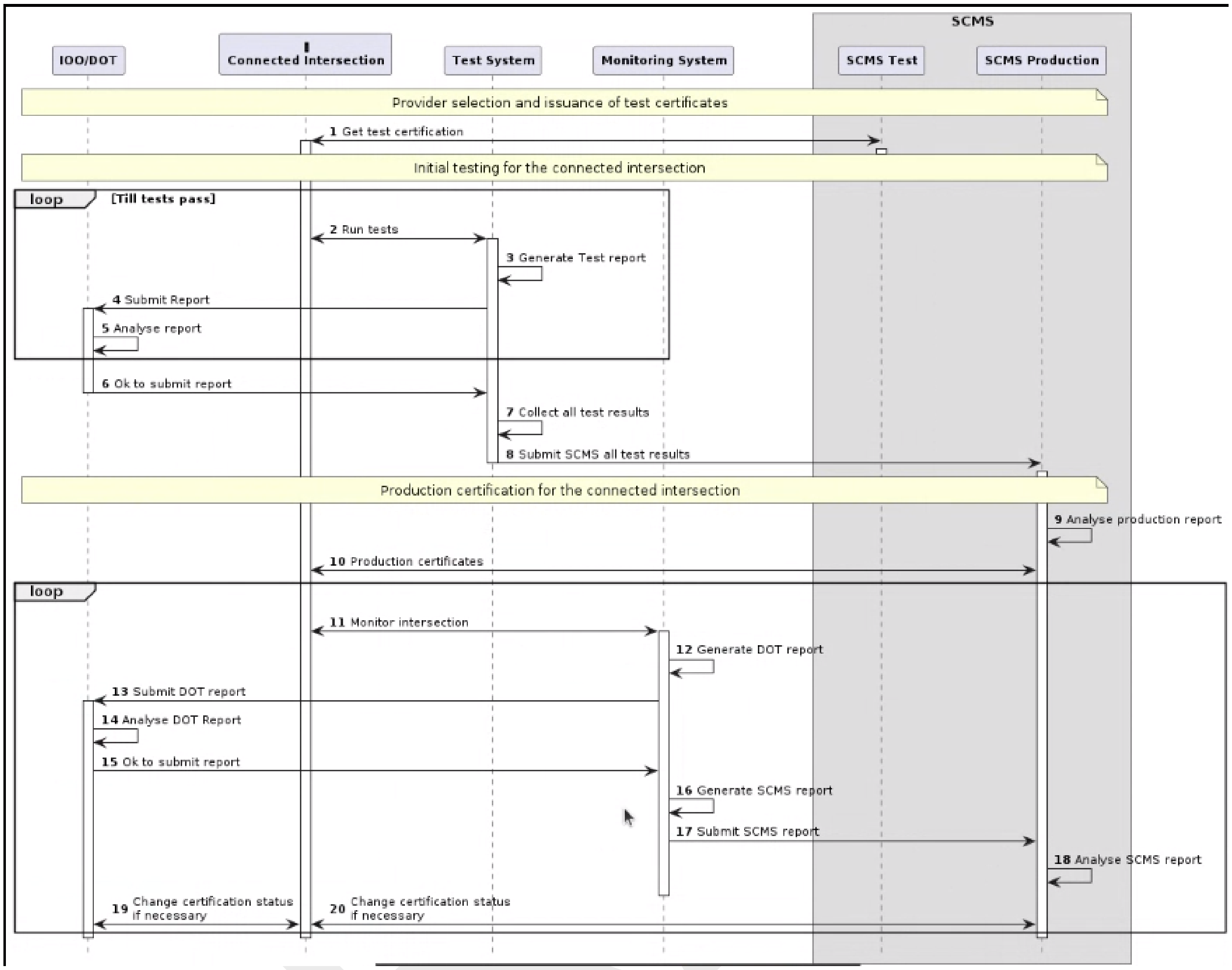

Figure B4 - Report flows[7]

[7] SCMS Manager – CI Test Results Report Format. SCMS Manager LLC via U.S. Department of Transportation.