SURFACE VEHICLE RECOMMENDED PRACTICE

CTI 4501™/3

PropDft JAN2026

Issued Proposed Draft 2026-01-06

Connected Intersections Implementation Guide - Security Guidance

RATIONALE

The Connected Intersections (CI) Implementation Guide 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 Infrastructure Owner Operators (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, this recommended practice focuses on harmonizing the messages broadcasted by a connected intersection.

This document focuses on requirements, design guidance, and testing considerations to address security needs and capabilities at connected intersections, providing practical guidance on protecting the trustworthiness of data sources and communications, ensuring reliable signal controller information, managing time sources, and validating key messages such as SPaT, MAP, and RTCM for authenticity, leading to interoperability and consistent, secure data exchange across different regions and deployments.

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 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 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 sub-documents. 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 an 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 sub-documents and other documents that support the implementation of a connected intersection. By separating out these focused topics, the guide more effectively supports IOOs, OEMs, suppliers, and application developers that 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.

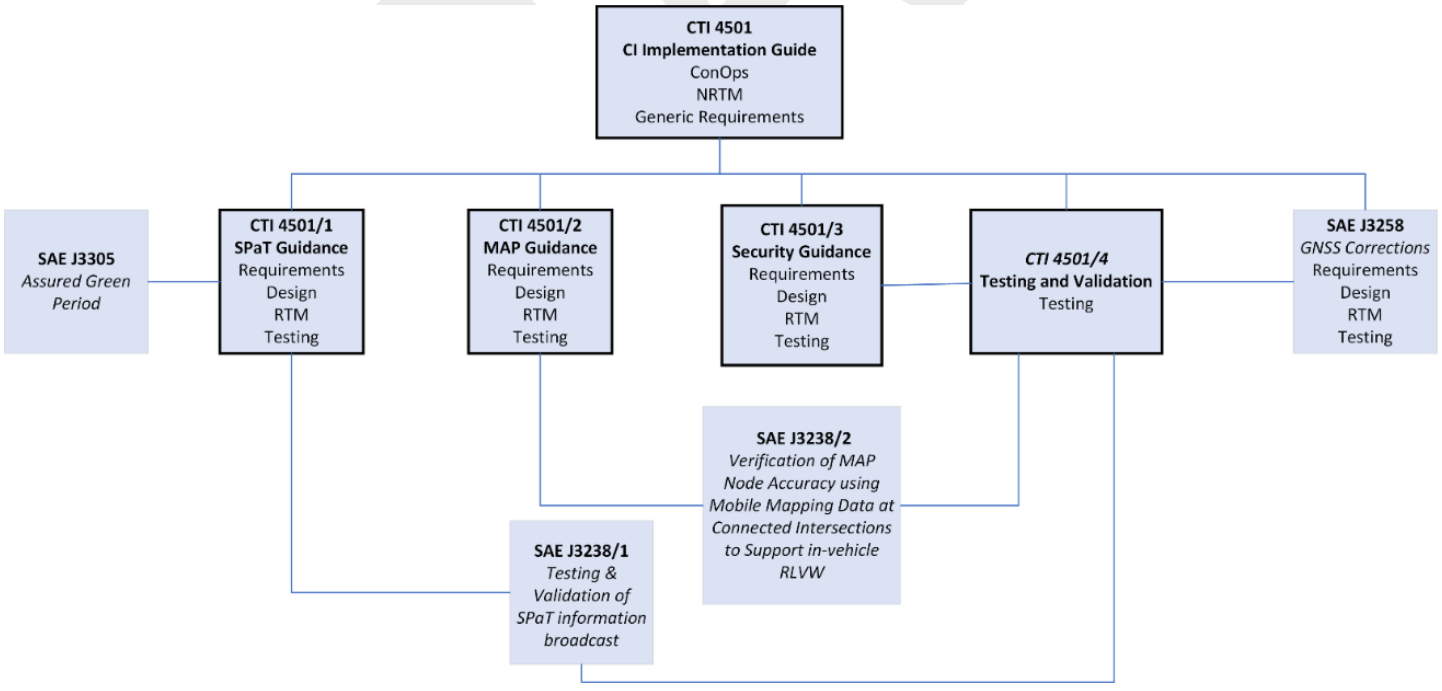

Figure 1 - Relationship with other documents

This Security Guidance document equips practitioners with targeted security guidelines, helping foster reliable, resilient connected intersections that maintain public trust and support the broader goals of interoperable, secure connected intersections. The document addresses multiple facets of security, while aligning with the overall structure and methodology of the main CTI 4501 document, including:

- Data Trustworthiness - Ensuring the integrity and authenticity of information originating from both infrastructure and vehicles.
- Communications Security - Protecting data exchanges across all relevant interfaces.
- System Management and Recovery - Defining best practices for updates, operational modes, and restoration procedures.
- Verification Requirements - Outlining checks to confirm that security measures are properly implemented.

For IOOs, this document provides actionable guidance on specifying and deploying security capabilities and functions to support robust, trustworthy connected intersections. For OEMs and developers, it explains how to secure the data and messages which will be broadcast from interoperable intersections, enabling the development of safety-critical applications such as RLVW.

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: 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 J2945/1 On-Board System Requirements for V2V Safety Communications

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 J3258 V2X Infrastructure Support for GNSS Corrections

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

SAE J3287 V2X Misbehavior Reporting

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

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

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 610.12 IEEE Standard Glossary of Software Engineering Terminology

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

2.1.4 ISO Publications

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

ISO/IEC/IEEE 24765 Systems and software engineering - Vocabulary

2.1.5 National Academy of Sciences Publications

Available at https://www.trb.org/OperationsTrafficManagement/Blurbs/173121.aspx.

Signal Timing Manual

2.1.6 NIST Publications

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

NIST FIPS 140-2 Security Requirements for Cryptographic Modules

2.1.7 NTCIP Standards

Available from NTCIP Coordinator, National Electrical Manufacturers Association, 1300 N. 17th Street, Suite 900, Rosslyn, Virginia 22209-3801, https://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

2.1.8 U.S. Department of Transportation, National Transportation Library Publications

Available from U.S. Department of Transportation at https://www.transportation.gov/.

CAMP protocols Security Credential Management System Proof-of-Concept Implementation: EE Requirements and Specifications Supporting SCMS Software Release 1.2.2

MUTCD Manual on Uniform Traffic Control Devices for Streets and Highways

2.1.9 Other Publications

Cooperative Automated Transportation Clarifications for Consistent Implementations (CCIs) for Connected Signalized Intersections

CIS Controls Implementation Guide for Industrial Control Systems

2.2 Related Publications

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

2.2.1 SAE Publications

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

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

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: https://www.ite.org/technical-resources/standards/rsu-standardization/.

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

2.2.3 Connected Vehicle Pooled Fund Study Publications

Available at https://engineering.virginia.edu/labs-groups/cvpfs.

CVPFS Connected Intersection Guidance Document

CVPFS CIMMS Systems Requirements

CVPFS Guidance Document for MAP Message Preparation

2.2.4 Crash Avoidance Metrics Partners (CAMP) Publications

Available from CAMP LLC at https://www.campllc.org/publications/.

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

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

2.2.5 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 802.11 IEEE Standard for Information technology - Telecommunications and information exchange between systems local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

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

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

2.2.6 Internet Documents

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

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

IETF RFC 6353 Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)

IETF RFC 8446 The Transport Layer Security (TLS) Protocol

2.2.7 ISO Publications

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

ISO 26262 Road vehicles - Functional safety, International Standards Organization

ISO/PAS 21448 Road vehicles - Safety of the Intended Functionality

2.2.8 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

2.2.9 NTCIP Standards

Available from NTCIP Coordinator, National Electrical Manufacturers Association, 1300 N. 17th Street, Suite 900, Rosslyn, Virginia 22209-3801, https://www.ntcip.org.

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

NTCIP 9001 The NTCIP Guide

2.2.10 RTCM Standards

Available from the Radio Technical Commission for Maritime Services, 2200 Wilson Blvd., Suite 102-109, Arlington, VA 22201, https://www.rtcm.org/publications.

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

2.2.11 SCMS Manager Publications

Available from SCMS Manager at https://www.scmsmanager.org/publications/.

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

2.2.12 U.S. Department of Transportation Publications

Available from U.S. Department of Transportation at https://www.transportation.gov/.

RSU Specification 4.1 Dedicated Short-Range Communications Roadside Unit Specifications v4.1, USDOT, Saxton Transportation Operations Laboratory

Accelerated Vehicle-to-Infrastructure (V2I) Safety Applications System Requirements Document, FHWA-JPO-13-059, July 18, 2012

Systems Engineering for ITS

2.2.13 Other Publications

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

3. DEFINITIONS

For the purposes of this recommended practice, the following definitions shall apply:

APPROACH: All lanes of traffic moving toward 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 eastbound 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

APPROACH SPEED: The uninterrupted speed (or free-flow speed) of through movement vehicles used in the design of the timing parameters that control the operations of the traffic signal.

ASSURED GREEN END TIME (AGET): The UTC time denoting the end of a green signal indication for a movement. The AGET is set when the CI/TSC infrastructure determines when the through movement green interval will definitively end, unless there is preemption, failure, or something else outside of the CI/TSC infrastructure’s control.

ASSURED GREEN PERIOD (AGP): When a connected vehicle is approaching a connected intersection in a through lane currently in a green signal state indication, the AGP is a fixed portion of green interval for the through movement that, when combined with the duration of the yellow change interval, decreases the likelihood that the vehicle will be in the connected intersection during a red signal state indication.

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

CI DATA ACTIVITIES: Creation and processing of CI data (including generating and signing the V2X messages).

CI DATA COMMUNICATIONS: Any transfer of CI data from one CI data entity to another. CI data communications are subject to security requirements specified in this document.

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

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

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

CONNECTED INTERSECTION (CI): An infrastructure system that creates and broadcasts signal, phase, and timing (SPaT), mapping information, and position correction data to Onboard 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.

CONNECTION: In the context of a connected intersection, the link between an ingress lane and a downstream lane, which may be an egress lane out of the intersection or an ingress lane within the intersection (e.g., storage lane).

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. It is typically used for control, configuration, and interface definition and is 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.

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.

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

PERMISSIVE MOVEMENT: A permitted movement that may conflict with protected movements and other permissive movements. Traffic making a permissive movement must yield to conflicting traffic and may be required to first come to a full stop.

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

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

PROTECTED MOVEMENT: A permitted movement that has the right of way and may conflict with permissive movements. Traffic making a protected movement must watch for conflicting traffic.

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

PROVIDER SERVICE IDENTIFIER: An integer that identifies an application specification. Source: SAE J3268

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

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

RLVW DETECTION ZONE (RDZ): The area on a through movement lane that is used to detect vehicles for the RLVW operation. The RDZ is upstream from and adjacent to the stopping distance to the stop line with a width equal to that of the lane and a length equal to 0.5-second approach speed.

ROADSIDE UNIT (RSU): A transportation infrastructure communications device located on the roadside that provides V2X connectivity between OBUs/MUs and other parts of the transportation infrastructure, including traffic control devices, traffic management systems, and back-office systems.

NOTE: Devices that are not part of the transportation infrastructure, such as cellular base stations or satellites, are not RSUs. Source: CTI 4001

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

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

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

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

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

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

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

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

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.

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.

TRUSTWORTHINESS: A property of a system that it is difficult for its data or behavior to be improperly altered; a property of data that, with high likelihood, it has not been improperly altered.

NOTE: This definition of trustworthiness is security-centric. Broader definitions are possible that capture the concept that the unaltered data is, with high likelihood, correct for the purpose for which it is intended. This document uses the narrower concept because the focus of this document is on security.

TSC INFRASTRUCTURE: The systems and components within the transportation field 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 document does not include networked communications or commercial connected vehicle applications. Source: SAE J3161 and SAE J3161/1

VULNERABLE ROAD USER (VRU): A term applied to those most at risk in traffic, i.e., those unprotected by an outside shield. VRUs are pedestrians (especially children, seniors, and people with disabilities), bicyclists, and motor cyclists. Source: CTI 4001

4. ABBREVIATIONS

AASHTO	American Association of State Highway and Transportation Officials
ACL	Access Control List
AGET	Assured Green End Time
AGP	Assured Green Period
ARC-IT	Architecture Reference for Cooperative and Intelligent Transportation
ASN.1	Abstract Syntax Notation 1
CA	Certificate Authority
CCI	Clarifications for Consistent Implementations (document)
CI	Connected Intersection
ConOps	Concept of Operations
CORS	Continuously Operating Reference Station
CPMS	Connected Intersection Performance Monitoring System
CRL	Certificate Revocation List
CTL	Certificate Trust List
CV	Connected Vehicle
CVPFS	Connected Vehicle Pooled Fund Study
DTLS	Datagram Transport Layer Security
ECLA	External Control Local Application
FCC	Federal Communications Commission
FHWA	Federal Highway Administration
FO	Functional Object
GNSS	Global Navigation Satellite System
HSM	Hardware Security Module
ICD	Interface Control Document
IEEE	Institute of Electrical and Electronics Engineers
IOO	Infrastructure Owner/Operator

IPSec	Internet Protocol Security
ITE	Institute of Transportation Engineers
LTE-V2X	Long-Term Evolution-Vehicle to Everything
MTBF	Mean Time Between Failures
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
O&M	Operations & Maintenance
OBU	Onboard Units
OEM	Original Equipment Manufacturers
ProSe	Proximity Services
PSID	Provider Service Identifier
RDZ	RLVW Detection Zone
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
RTM	Requirements Traceability Matrix
SAE	SAE International
SCMS	Security Credential Management System
SDO	Standards Development Organization
SEP	Systems Engineering Process
SPaT	Signal Phase and Timing
SSL	Secure Sockets Layer
TLS	Transport Layer Security

TMS	Traffic Management System
TSC	Traffic Signal Controller
TSCBM	Traffic Signal Controller Broadcast Message
USDOT	United States Department of Transportation
V2I	Vehicle-to-Infrastructure
V2X	Vehicle-to-Everything
VRU	Vulnerable Road User

5. CONCEPT OF OPERATIONS

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

6. FUNCTIONAL REQUIREMENTS

This section defines the functional requirements based on the security user needs identified in the Concept of Operations (refer to CTI 4501, Section 5). This section includes the following:

a. A tutorial

b. Needs to Requirements Traceability Matrix (NRTM). A functional requirement is a requirement of a given function and therefore is only required to be implemented if the associated functionality (e.g., user need) is selected through the use of the NRTM. The NRTM also indicates which of the items are mandatory, conditional, or optional. The NRTM can be used by procurement personnel to specify the desired features for a connected intersection or can be used by an implementation to document the features supported by their implementation. The NRTM can also be used to define which requirements are to be tested (by demonstrating which requirements are to be implemented). The NRTM is in CTI 4501, 6.2.3, Table 5.

c. Requirements. These are requirements that collectively satisfy the user needs related to security in CTI 4501, 5.4.4, Security (Needs). These requirements provide the details so that user needs can be satisfied and validated.

Section 6 is intended for all readers, including the following:

a. Transportation Managers

b. Transportation Operators

c. Transportation Engineers

d. System Integrators

e. Device Manufacturers

f. Application Developers

For the first four categories of readers, Section 6 is useful in understanding the details of CTI 4501. For these readers, 6.2.3 is particularly useful in preparing procurement specifications and assists in mapping the various rows of this table to the more detailed text contained within the other sections.

For the next two categories of readers, this section is useful to fully understand what is required for conformance to CTI 4501. Table 5 in CTI 4501, 6.2.3 may be used to document the capabilities of their implementations.

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

6.1 Tutorial [Informative]

This Functional Requirements section defines the formal requirements that are intended to satisfy the user needs identified in CTI 4501, 5.4, Needs. This is achieved through the development of an NRTM that traces each user need to one or more requirements defined in this section. The details of each requirement are then presented in 6.3.

6.2 Needs to Requirements Traceability Matrix (NRTM)

Refer to CTI 4501, 6.2 for the Needs to Requirements Traceability Matrix.

6.3 Requirements

The requirements for CTI 4501/3 follow.

Some requirements are generic requirements for a CI system, and this section references those requirements in CTI 4501. Some requirements are not applicable to security (and are marked as not applicable), but the requirements heading are included in this section so the numbering is consistent among CTI 4501 and the companion documents of CTI 4501/3 (e.g., CTI 4501/1).

6.3.1 Architectural Requirements

Refer to CTI 4501, 6.3.1 for the Architectural Requirements. This section contains the requirements for wireless communications between a connected intersection and the applications on an OBU/MU.

6.3.2 TSC Infrastructure to RSU Requirements

Not applicable.

6.3.3 Message Requirements

Not applicable.

6.3.4 Security Requirements

The security requirements for a connected intersection follow.

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

The following terms are used for Security Requirements:

- **"Inside the CI" versus "Outside the CI."** A component that the connected intersection controls physical and logical access to is “inside the CI.” A component that the connected intersection does not control access to is "outside the CI." For components in a definitionally gray area (e.g., virtual machines running in the cloud, where the connection intersection controls logical access but not physical access, and where in this case "physical access" is not clearly defined), common sense, i.e., a sense of whether or not the CI organization in practice controls access to the component, should be used as to whether a component is inside or outside the connected intersection.

- **"Ensure that"** means that a failure of the system to have the property X is inconceivable. If a property needs to be "ensured," then a connected intersection must provide that property or it cannot be validated. If a property is important but does not need to be "ensured" in this sense, the document uses "have mechanisms to provide assurance that. "

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

- **"CI data activities"** means creation and processing of CI data (including generating and signing the V2X messages).

- **"Manually entered CI data"** is any CI data that is entered by a human. This can include updates to configuration files, etc.

- **"Manual CI data sources"** are any CI component on which CI data is entered by a human.

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

- **"CI data communications"** means any transfer of CI data from one CI data entity to another. CI data communications are subject to security requirements specified in this document.

- **IMPORTANT:** Because of how position and time are obtained from GNSS information, a GNSS data source (i.e., a system of GNSS satellites talking to a receiver inside the connected intersection) cannot be subject to all the security requirements below when used for position and timing information. This is indicated explicitly in the security requirements below by use of the phrase "EXCEPTION: GNSS data sources are not subject to this requirement." Other time and position sources are subject to all of the data source requirements in this document.

  The rationale for making exceptions specifically for GNSS sources is that, while in general it is appropriate to require cryptographic communications security on CI communications, in the specific case of GNSS, the exact time of arrival of GNSS signals is a key piece of information in determining time or position. Since this cannot be cryptographically protected, it does not make sense to require some of the security requirements below around cryptographic message protection to apply to some GNSS transmissions. (It is also the case that most GNSS systems haven't even implemented cryptographic message protection, for exactly this reason, and so having it as a requirement would prevent the use of those GNSS systems.)

- **"CI data entities"** are the entities involved in creating and processing CI data. They may be inside or outside the connected intersection. The following types of data entities are defined in this section and have different requirements associated with them.
    - Data sources
        - Manual data sources
        - Automated data sources
        - External data sources
    - Data processing components
        - Internal data processing components
        - External data processing components
    - "Encoded V2X Message Production" components, which produce encoded V2X messages
    - V2X Message signing components, which create signatures on V2X messages
    - V2X Transmission components, which transmit the V2X messages
    - Monitoring and logging components

    Figure 2 shows the different components and the order in which they are used during the creation and transmission of a V2X message. Note that V2X message production and signing can be considered special cases of data processing; they are separated from the other cases of data processing due to their specialized role in the V2X message sending system. Note also that, other than message production and signing components, the use of data processing components is optional and a system architecture could simply transport data from its source to the relevant V2X message production component such that there is no other component where additional data processing takes place. Note also that the monitoring and logging systems can be considered CI data sources and/or CI data processing components but are separated in this diagram because they do not directly impact message payloads.

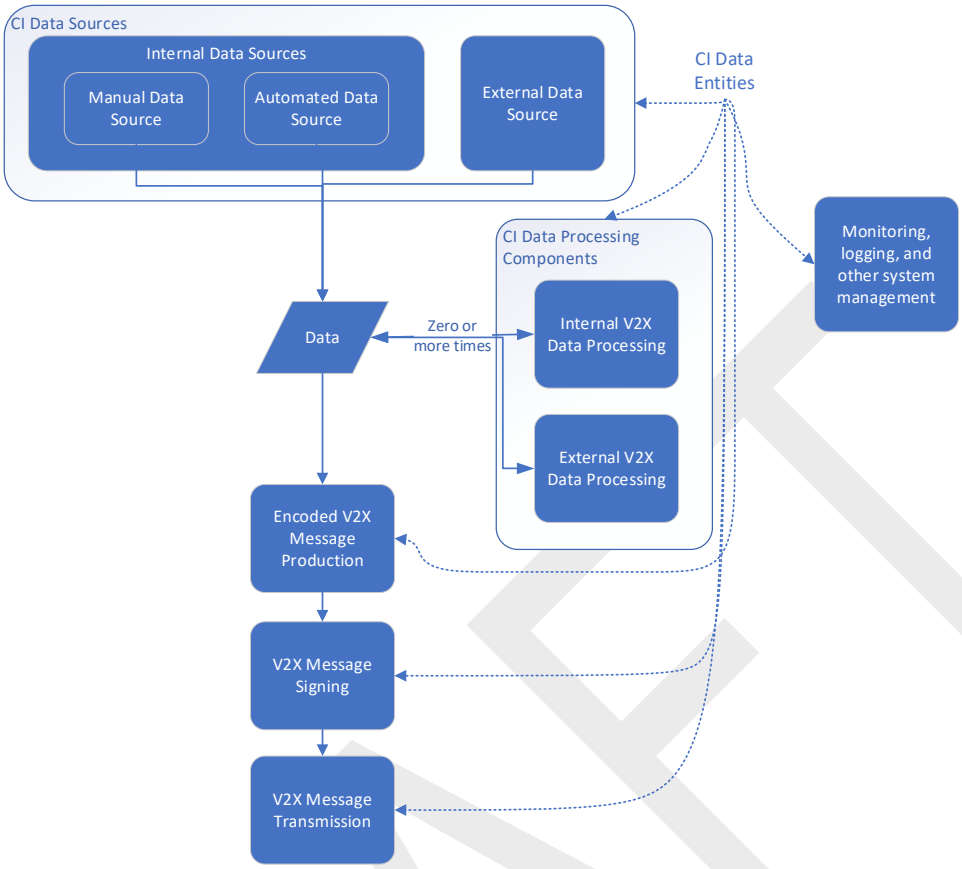

Figure 2 - CI data entities plus information flow when creating V2X message

- **Self-monitoring and logging.** See Figure . Each component has a self-monitoring system that writes to its local logging system. Local logs are available to the central logging system, and the diagnostics system can report directly to central diagnostics without having to go via the logs.

  This model considers the logging system as a subsystem of the monitoring system and in particular talks about the logging system as logging information provided to it by the monitoring system (in other words, anything that causes information to be logged is definitionally part of the monitoring system). This is not intended to require a particular architecture or distribution of functions between "logging processes" and "monitoring processes" on the component. If on a particular component there is a system named "monitoring system" and another system named "logging system," and there is also some information provided to the logging system by a process other than the specific process named "monitoring system," that's not in contradiction with this document.

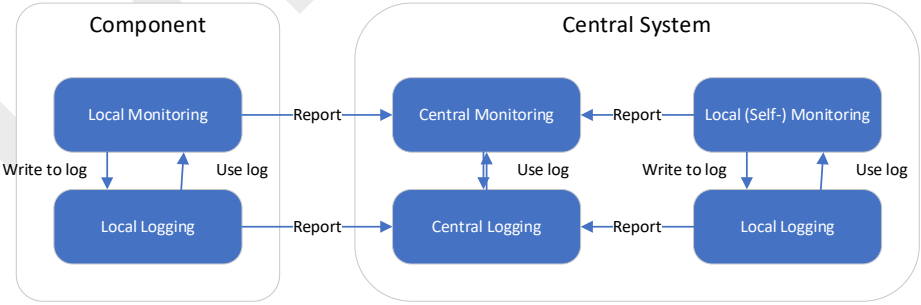

Figure 3 - Diagnostics and monitoring entities

A functional diagram that also identifies data processing roles is shown in Figure .

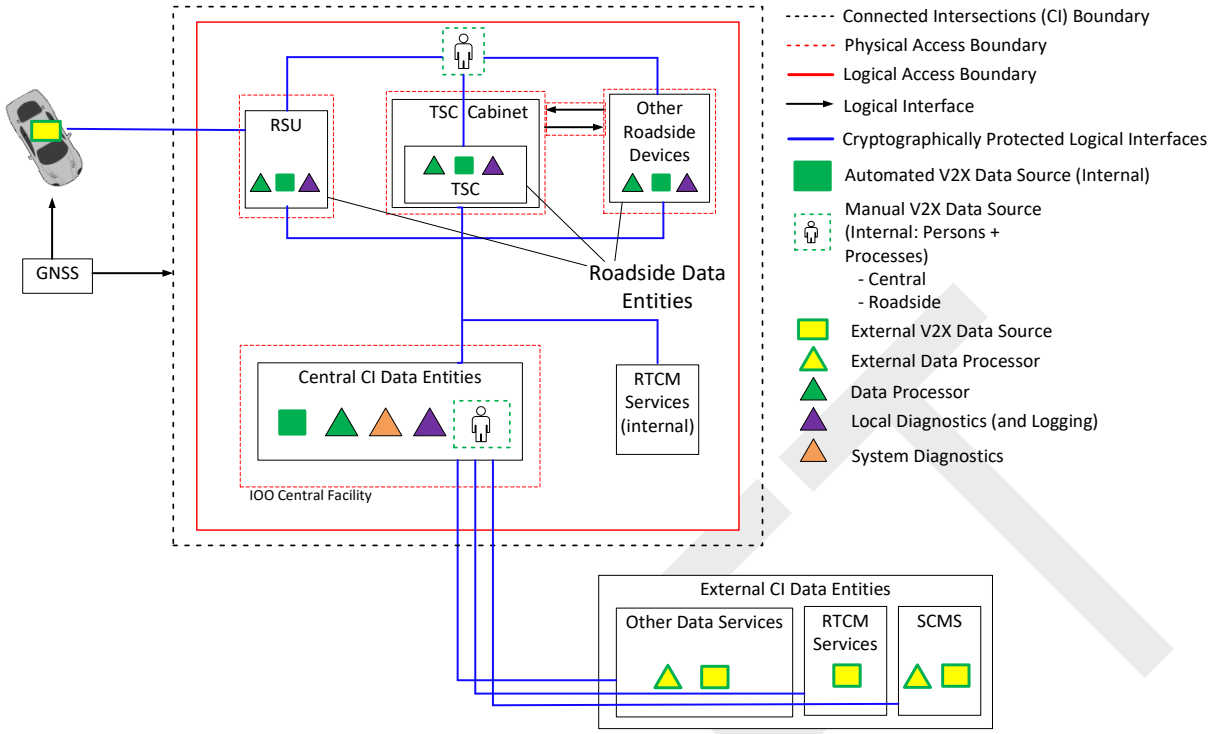

Figure 4 - Application-specific functional roles

6.3.4.1 Data Trustworthiness: Sources and Processing

The requirements for sources and processing data trustworthiness for a connected intersection follow.

6.3.4.1.1 Internal Data Sources and Processing

A connected intersection shall maintain an up-to-date list of all CI data entities, i.e., all components inside the connected intersection that (a) provide CI data, (b) modify or transform CI data, (c) generate encoded V2X messages, (d) sign encoded V2X messages, or (e) transmit V2X messages.

Per the definition of CI data, CI data includes not just information that directly affects the V2X messages but also information that affects the operation of the system such as configuration files, diagnostics and logging information, security certificates, software updates for CI data entities, etc. The list of CI data entities shall include all components in the system that source or process any kind of CI data.

NOTE: See the discussion above about how GNSS data sources are exempt from some of the security requirements below. These exceptions for GNSS data sources are noted explicitly wherever they apply.

6.3.4.1.2 Manual Data

A connected intersection shall maintain a list of all CI data that is entered manually, i.e., by a process involving human input. This covers all CI data including, for example, configuration information (per 6.3.4.1.1).

6.3.4.1.3 Internal Manual Data Sources

A connected intersection's list of CI data entities shall identify all manual data sources, i.e., all components where CI data is entered manually.

NOTE: This document distinguishes between manual and non-manual/automated data sources for internal CI data sources because there are specific security requirements on manual data sources. For external CI data sources, whether they are manual or non-manual does not affect the security requirements stated in this document, and so the distinction does not apply.

6.3.4.1.4 Permitted Data from Manual Data Sources

For each manual data source, the connected intersection shall identify which CI data it is permitted to enter. This is intended to capture cases such as when employee phones allow updating diagnostics tickets but not the entering of MAP speed limit data. The intent is for the connected intersection to be aware of systems that have some level of access to the CI system so that it can implement mechanisms to prevent privilege escalation attacks and similar.

The list of data that the source is permitted to enter will also define the data that the source is not permitted to enter. This is the subject of subsequent security requirements. The list will ideally identify all the individual systems on which data could be entered but is not allowed to be. However, it may contain descriptions that identify multiple systems, e.g., "all machines in room C101," as long as the description is correct and is clear to a person with a reasonable level of familiarity with the CI system (e.g., it could be used by an external auditor assisted by someone who works in the relevant part of the CI).

6.3.4.1.5 External CI Data Entities

A connected intersection shall maintain an up-to-date list of CI data entities outside the connected intersection, i.e., entities that provide data that is used to generate V2X messages or that modify or transform data used to generate V2X messages including, for each external data source, the CI data that it provides.

This list of data sources need only include the "final external data sources," i.e., the systems to which the CI systems directly connect to obtain the data. It does not need to include any other components outside the connected intersection that affect the data because the connected intersection is concerned only with the data directly provided to the connected intersection.

External data processors are data processors where data is under the control of the connected intersection and is then passed out of the control of the connected intersection for processing and is then received back by the connected intersection and made use of. (If the connected intersection doesn't control the data before passing it to the processor, the processor is just considered an external data source per the previous note). It is very unlikely that SPaT messages will use external data processors, but it is conceivable that it might happen for MAP or RTCMcorrections. In a connected intersection's architecture, there may be no external data processors at all, i.e., no flows where information flows out, is modified, and then flows back in. If this is the case, there are no risks from external data processors, and all risks and requirements described below regarding external data processors do not apply.

Senders of received V2X messages are external data sources for the purposes of this requirement and as such are subject to the requirement to be listed. The list of external data sources cannot include each individual vehicle in the world that might send V2X messages. For V2X senders, this requirement can be met by listing all of the components within the connected intersection that receive V2X messages from senders outside the connected intersection (the expectation is that this will be all the CI's RSUs), noting that they are V2X message receivers. If the CI operator considers it appropriate to provide more detail in the list (for example, if the operator decides that there are different types of Basic Safety Message [BSM] senders and that it is possible and useful to distinguish them), then the CI operator can provide that detail at their discretion.

The source for assigning intersection identifiers is a data source for the purposes of this requirement and may be inside or outside the connected intersection (although in most CI systems, it can be expected to be inside the connected intersection). As such, the source for assigning intersection identifiers is subject to the requirements below. Additional requirements are in 6.3.4.12.

NOTE: GNSS sources are external data sources for the purposes of this requirement and should be listed, although they are not subject to some of the security requirements below. See above for further discussion.

6.3.4.1.6 Authorized CI Data Entities

A connected intersection shall only use data from authorized CI data entities, i.e., entities for which it has been established that they are permitted to connect to the connected intersection for an identified set of CI data activities (or to be precise, entities whose communications can be reliably determined to come from an entity with such authorization; i.e., authorized entities that are authenticated per 6.3.4.7).

The proof that an entity is authenticated is established via the communications security mechanisms specified in 6.3.4.2, Data Communications Security. The exception for time sources is given because many useful time sources do not support cryptographic or other proof that they are authorized.

For received V2X messages, this requirement is fulfilled by requiring the received V2X messages to have a valid IEEE Std 1609.2 signature. See 6.3.4.4.

EXCEPTION: GNSS data sources are not subject to this requirement.

6.3.4.1.7 Authenticated CI Data Entities

A connected intersection shall only use data from authenticated CI data entities. For received V2X messages, this requirement is fulfilled by requiring the received V2X messages to have a valid IEEE Std 1609.2 signature. See 6.3.4.4.

EXCEPTION: GNSS data sources are not subject to this requirement.

6.3.4.1.8 Integrity of Operations for Internal CI Data Entities

A connected intersection shall ensure that mechanisms are implemented to protect the integrity of operations for internal CI data entities.

Functional controls on the component that provide integrity of operations include secure boot, self-test on power on, and other design choices to provide assurance that a component is in a correct state. This requirement also covers active cybersecurity controls such as firewalls, intrusion detection, blocking ports against sniffing, etc. Organizational controls include keeping a record off-device of the hardware and software configuration of the component and ensuring it is correct. See 6.3.4.14 for organizational controls.

6.3.4.1.9 Integrity of Operational Mode for Internal CI Data Entities

A connected intersection shall protect a CI data entity from operating in or transitioning to any of the following modes when it should not:

- Normal Mode or test mode (refer to CTI 4501, 6.3.5.3.1, Support Normal Mode)
- Maintenance Mode (refer to CTI 4501, 6.3.5.3.2, Maintenance Mode)
- Any mode other than Normal Mode or Maintenance Mode

6.3.4.1.10 Integrity of Operational Mode Indications for Internal CI Data Entities

A CI data entity shall implement mechanisms to protect itself from incorrectly indicating its operational mode or status.

6.3.4.1.11 Physical Access to Internal CI Data Entities

A connected intersection shall physically secure and control access to all CI data entities inside the connected intersection.

NOTE: See "inside the CI" in 6.3.4. If a component is naturally considered to be "inside the CI" but the connected intersection does not have physical control of access to that component, this requirement does not apply to that component.

6.3.4.1.12 Physical Access to Internal CI Data Entities During Outages or Degraded Operations

A connected intersection shall ensure that the physical access control mechanisms to CI data entities are effective during power outages or disruptions, degraded operations, or other error states.

This is implied by 6.3.4.1.11 but is stated explicitly for clarity. See 6.3.4.14.

6.3.4.1.13 Logical Access to Internal CI Data Entities

A connected intersection shall logically secure and control access to CI data entities inside the connected intersection.

NOTE 1: See the discussion of "inside the CI" in 6.3.4. It is conceivable that there are CI data entities inside the CI that only have physical access protection and do not have "logical access" at all (e.g., sensors that output data as a one-way flow but cannot be "programmed," e.g., induction loops). This requirement does not apply to components that do not have logical access (as if it doesn't exist it can't be secured).

NOTE 2: This requirement is intended to capture an intent that all CI data entities, especially those that are outside an access-controlled facility (e.g., RSUs, signal controllers, etc.) follow best common practices to protect against intrusion or "pwning." Typical best practice techniques include: restrict boot-time access to internal shells or recovery environments unless authenticated; audit and monitor physical access paths (UART, SD card, USB) for potential attack vectors; use cryptographic signatures on firmware that are checked before boot; filesystem integrity checks; disable unused interfaces such as UART, USB, or SD card access unless explicitly needed and disable debug interfaces; and restrict access to EFI or recovery shells using passwords or a similar mechanism. The CI operator is expected to apply these or similar techniques so as to mitigate security threats but judiciously such that recovery paths from failure states are still possible.

6.3.4.1.14 Logical Access to Internal CI Data Entities During Outages or Degraded Operations

A connected intersection shall ensure that the logical access control mechanisms to CI data entities are effective during power outages or disruptions, degraded operations, or other error states.

This is implied by 6.3.4.1.13 but is stated explicitly for clarity. See 6.3.4.14.

6.3.4.1.15 Mitigate Malicious Access to Internal CI Data Entities

A connected intersection shall implement mechanisms (technical or procedural) to mitigate residual risks arising from unauthorized physical or logical access to CI data entities inside the connected intersection, if any such significant risks are identified.

The risk arising from unauthorized access to an internal CI data entity will typically be that that data entity sends incorrect data. Security requirements in 6.3.4.2 (for the general case) and in other sections (for specific cases to do with specific V2X messages) address the impact of incorrect data. If all of those requirements are fulfilled, this requirement can be fulfilled by documenting that those requirements have been fulfilled.

NOTE: In the above requirement, "significant" is deliberately not precisely defined. The definition used by an individual connected intersection may be specific to that connected intersection within constraints set by law, regulation, SCMS policy, etc. For further discussion, see 7.3.4.1.

6.3.4.1.16 Access Control on Internal CI Data Entities During Life Cycle

A CI data entity shall maintain appropriate access control during all of the following life cycle phases:

- Initial installation
- Maintenance or degraded operations
- System updates
- Software/firmware updates
- System outages
- Removal/decommissioning
- Performing security management on a CI data entity
- Entering or leaving a Maintenance Mode
- Power outages
- Recovery from disruption

"Appropriate access control" can include being inaccessible until the CI data entity transitions out of the current state.

6.3.4.1.17 Integrity of Operations for External CI Data Entities

A connected intersection shall obtain assurance that mechanisms are implemented to protect the integrity of operations for external CI data entities.

"Integrity of operations" includes secure boot, self-test on power on, and other design choices to provide assurance that a component is in a correct state.

The connected intersection might obtain this assurance by directly corresponding with the operator of the external CI data entity or might obtain it by reviewing statements made by the operator and getting assurance that way. For example, for GNSS systems, it is public knowledge that the operator of the system includes mechanisms to protect the integrity of operation of the system. In these cases, this requirement can be fulfilled by documenting integrity of operation as "public knowledge."

6.3.4.1.18 Mitigate Malicious Access to External Data Sources and Processing

A connected intersection shall identify and, where appropriate, implement mechanisms (technical or procedural) to mitigate risks arising from unauthorized physical or logical access to CI data entities outside the connected intersection.

It is possible that the risks are so low (due to good access controls known to the CI or low impact of incorrect data from that data source) that no mitigation is necessary. If this is the case, this requirement is fulfilled by documenting that no mitigation is necessary for that data source.

The risk arising from unauthorized access to an external CI data entity will typically be that that data entity sends incorrect data. Security requirements in 6.3.4.2 (for the general case) and in other sections (for specific cases to do with specific V2X messages) address the impact of incorrect data. If all of those requirements are fulfilled, this requirement can be fulfilled by documenting that those requirements have been fulfilled.

Senders of received V2X messages are external data sources for the purposes of this requirement and as such are subject to the requirement that risks are mitigated. Informally, the risk can be considered mitigated by determining that the V2X message is validly signed per IEEE Std 1609.2 (note that "validly signed" includes checking for revocation, etc.). The receiver can also optionally carry out misbehavior detection on received messages. Section 6.3.4.2.12 provides more detail on appropriate mitigations. Further detail is provided in the design section.

6.3.4.1.19 Access Privileges for Data Sources and Processing

A connected intersection shall associate specific physical and logical access privileges to users on a role or identity basis that govern their access to internal CI data entities, including managing the actions that that user is allowed to perform on or using that CI data entity. This includes identifying administrator roles for each CI data entity and assigning the administrator role to specific individuals (directly or by association with a system role).

6.3.4.1.20 Access Privileges for Manually Entered Data

A connected intersection shall associate specific physical and logical access privileges to users on a role or identity basis that govern their ability to enter each identified type of manually entered data.

These privileges could be applied by a rule rather than by a list. For example, "everyone who has access to the speed limit database has permission to update the speed limits given in a MAP."

The reference to "each identified type of manually entered data above" is meant to indicate that for all types of data it must be clear who has privileges to enter it. It is not necessary to have a specific list for each of the identified types of data; the connected intersection can use names for groups of data types, e.g., "all MAP information" or "SPAT configuration files."

Manual data sources are data sources and subject to all other security requirements that apply to data sources, e.g., 6.3.4.1.13.

6.3.4.1.21 Record of Accesses to CI Data Entities

A connected intersection shall maintain an auditable record of accesses to CI data entities inside the CI. This record shall identify the identity of the accessor, which may be an individual, an account identifier, or some other identity provided, as part of the access.

NOTE: This is optional because a connected intersection will probably be able to recover from a compromise without needing this record, and so this record is not required for operational robustness (although it is likely to be useful, especially in preventing subsequent compromises, and so its use is recommended).

6.3.4.1.22 Detect Data Injection from Unauthorized CI Data Entities

A connected intersection shall detect unauthorized CI data entities, inside or outside the CI, that are attempting to cause their data to be used to generate or modify CI data, including V2X messages.

NOTE: This is optional because so long as the connected intersection will only use data from authorized CI data entities (per 6.3.4.2.3, 6.3.4.2.7, 6.3.4.2.8, and 6.3.4.2.9), the outputs are protected. However, it is good practice to have an intrusion detection system that will detect attacks of this type.

6.3.4.1.23 Self-Monitoring for Internal CI Data Entities: Detect Significant Errors

A connected intersection shall identify and implement mechanisms such that CI data entities inside the connected intersection run self-monitoring such that operational errors that significantly affect CI data, including errors that affect the integrity of stored digital information such as executable code and stored data, are detected in a timely manner.

This requirement could be addressed for a particular component by stating that no such mechanisms have been identified as necessary for that component because external monitoring provides sufficient coverage of errors.

"Significant[ly]" and "timely" are deliberately not precisely defined. The definition used by an individual CI may be specific to that CI within constraints set by law, regulation, SCMS policy, etc. For further discussion, see the design section.

Monitoring information counts as CI data per the definition of CI data, and so access to the diagnostic information on the component is subject to the access control and other data-related security requirements of this section.

See 6.3.4.14 for system-wide diagnostics requirements.

6.3.4.1.24 Events to be Monitored by Self-Monitoring

For each CI data entity inside the connected intersection, the events covered by self-monitoring shall include the following if applicable to that specific entity:

- Loss of network connection
- Loss of power to any individual components
- loss of input CI data
- loss of assurance that output data is being received
- Loss of signing certificate validity (because of expiry, revocation, or other reasons)
- Failures of integrity of operation (see 6.3.4.1.8)
- Integrity or authentication failures on CI data communications
- Integrity or authentication failures on software updates
- Failed user authentications, including excessive numbers of failed authentication attempts
- Access to - including modification or removal - system and device logs (including who/what performed the access)
- Attempts of operators to invoke or disable functions and services for which they are not authorized
- Modification of user/operator access rights and authenticators
- Excessive resource consumption events which may indicate a type of Denial-of-Service attack
- Modification of the diagnostic system's configuration
- Update of the CI data entity’s software or other configuration
- Interactions that are indicative of known cyberattacks
- Restarts or power cycles

Specific self-monitoring events for components with specific application roles are provided below.

6.3.4.1.25 Self-Monitoring for Internal CI Data Entities: Other System Monitoring

The self-monitoring system on a CI data entity shall provide monitoring of system properties and events beyond the requirements in 6.3.4.1.24, as considered appropriate by the CI operator.

NOTE: This is optional because the CI operator may not consider it important to monitor other events.

6.3.4.1.26 Self-Monitoring for Internal CI Data Entities: Robustness

A connected intersection shall identify and implement mechanisms such that the self-monitoring processes on CI data entities are robust against spoofing and other cyberattacks that would lead to them producing incorrect information.

In fulfilling this requirement, it is possible that the CI operator will determine that the default configuration of the monitoring system, running on a component that fulfills the security requirements in this section, is sufficiently robust and no additional mechanisms or configuration are necessary. If this is the case, then this requirement is fulfilled for that component.

"Incorrect information" in this context includes both detecting an error when there is no error and not detecting an error when there is an error.

Per 6.3.4.1.42 and 6.3.4.1.43, data created or modified by the self-monitoring system is required to be stored in a robust and integrity-protected way.

6.3.4.1.27 Self-Monitoring for Internal CI Data Entities: Error Management

A connected intersection shall implement mechanisms such that if a self-monitoring test for a CI data entity inside the connected intersection indicates an error that affects CI data, that component shall do at least one of (a) attempt to recover automatically; (b) notify a central monitoring system that will manage a central response such as notifying an operator; (c) directly notify an operator; (d) locally log the failure; (e) stop sending that CI data (including specific V2X messages if appropriate); and/or (f) inform receivers of that CI data that the data is not available or is suspect. Additional mitigations may also be implemented.

Monitoring information that is "reported out" per (b) above counts as CI data per the definition of CI data, and so the data communications for that information is subject to the data communications security requirements in 6.3.4.2.

Error states can be detected by means other than self-monitoring. Those means of detection, and associated security requirements, are addressed below.

6.3.4.1.28 Recovery from Failure for Internal CI Data Entities

For each CI data entity inside the connected intersection, the connected intersection shall have a plan to recover from error states and to validate that recovery has been successful for that component.

The error management approach may, but does not have to, depend on the specific error state.

See 6.3.4.13 for system-wide error recovery requirements.

6.3.4.1.29 Assurance of Recovery from Failure for Internal CI Data Entities

For each CI data entity inside the connected intersection that has a plan for recovery from an error state, the connected intersection shall implement mechanisms to provide assurance that the component does not incorrectly report its recovery state (recovered when not recovered or not recovered when recovered).

The mechanisms may, but do not have to, depend on the specific error state being recovered from.

6.3.4.1.30 Source Assurance for Recovery from Failure for Internal CI Data Entities

For each CI data entity inside the connected intersection that has a plan for recovery from an error state, the connected intersection shall implement mechanisms to provide assurance that reports of the recovery state are only accepted if they come from an authorized source.

For example: (a) this could be the output of a self-test from the component, using cryptographic authentication bound to that component; or (b) this could be a diagnostic report from trusted personnel. Other approaches are possible.

6.3.4.1.31 Automated Recovery from Failure for Internal CI Data Entities is Not to Be an Attack Vector

For each CI data entity inside the connected intersection that has a mechanism for automated recovery from an error state, the connected intersection shall (1) analyze the risk that the automated recovery mechanism can be maliciously misused and (2) mitigate any identified significant risks.

NOTE: In the above requirement, "significant" is deliberately not precisely defined. The definition used by an individual CI may be specific to that CI within constraints set by law, regulation, SCMS policy, etc. For further discussion, see the design section.

6.3.4.1.32 Self-Monitoring for Internal CI Data Entities: Logging

The self-monitoring system on a CI data entity shall include logging of system properties and events as considered appropriate by the CI operator, including events identified in 6.3.4.1.24 as applicable.

NOTE: This is mandatory but can be fulfilled for a particular CI data entity by determining that in that case there are no properties or events appropriate for logging.

6.3.4.1.33 Log Generation for External CI Data Entities

A connected intersection shall maintain a list of external CI data entities for which the connected intersection requires them to implement a log generation and log management capability, including identifying the information that is required to be logged by each.

A connected intersection is not required to impose a logging requirement on every external CI data entity, just to identify which external CI data entities are subject to that requirement. For example, GNSS data sources will not be required to implement logging.

6.3.4.1.34 Log Events for CI Data Entities

For each CI data entity that implements logging under 6.3.4.1.32 and 6.3.4.1.33, a connected intersection shall identify the conditions governing which events are to be logged (e.g., create a list of the types of events that are logged) and shall have mechanisms to update these conditions.

6.3.4.1.35 Changes in Logged Information

A connected intersection shall specify conditions under which the logging information gathered by a CI data entity (or any other logging activity carried out by a CI data entity) should be changed and implement mechanisms to effect that change when appropriate.

For example, if a component changes the data activities it is engaged in, it might be necessary to update what the component logs.

In particular, for external CI data entities that carry out logging, the connected intersection is expected to have a process to be aware of any changes in data activities by those entities and to update logging instructions appropriately.

6.3.4.1.36 Access to Logs for CI Data Entities

A connected intersection shall ensure that mechanisms are implemented by components for which logging is required under 6.3.4.1.32 and 6.3.4.1.33 to convey relevant log information to human and/or automated systems for analysis.

6.3.4.1.37 Timely Access to Logs for CI Data Entities

A connected intersection shall implement mechanisms to provide assurance that results of log and event data security analysis (for components for which logging is required under 6.3.4.1.32 and 6.3.4.1.33) are provided to authorized system administrators in a timely fashion.

NOTE: In the above requirement, "timely" is deliberately not precisely defined. The definition used by an individual CI may be specific to that CI within constraints set by law, regulation, SCMS policy, etc. For further discussion, see the design section.

6.3.4.1.38 List of Communications Nodes on which Data Could Be Modified

The connected intersection shall maintain an up-to-date list of components inside the connected intersection through which communications between CI data entities pass and for which the data is not cryptographically protected against modification by that component.

For example, if there is a component such that cryptographic protection is applied at layer 2 for incoming and outgoing communications and CI data passes through that component without any cryptographic protection having been applied at a higher layer, such that the component could in principle modify the CI data, then the component shall be included on this list.

This requirement applies to any component that CI data might pass through. It is not required that the CI data always passes through that component. If a connected intersection uses dynamic or conditional routing of information and there is a component as described above, such that the CI data plausibly might sometimes pass through that component, then that component should be on this list.

6.3.4.1.39 Communications Nodes on which Data is Manipulable Count as Data Transformation Components

If there are any components inside the connected intersection through which communications between CI data entities pass and for which the data is not cryptographically protected against modification for that component, then those components shall be considered internal CI data entities and are subject to all the relevant security requirements.

6.3.4.1.40 Availability of CI Data

For each internal CI data entity that receives data, the connected intersection shall evaluate the risk that the expected data is unavailable and the impact of that unavailability.

For specific data types (e.g., SPaT information), more specific requirements are provided later in the security requirements section.

6.3.4.1.41 Mitigate Failures of Availability for CI Data

For each internal CI data entity that receives data, the connected intersection shall implement mechanisms to mitigate risks arising from the unavailability of CI data.

For specific data types (e.g., SPaT information), more specific requirements are provided later in the security requirements section.

6.3.4.1.42 Storage Integrity for Internal CI Data Entities: Risk Assessment

For each internal CI data entity that makes use of CI data stored on that component, the connected intersection shall evaluate the risk that the stored CI data is modified prior to its use in creating V2X messages and the impact of such modification.

Following the evaluation, the combination of access control and other security requirements in this section might be considered secure enough to make the risk of data modification negligible. The point of this requirement is to encourage CI deployers to double-check that there aren't any remaining vulnerabilities after those security requirements are implemented and to identify if there is any operationally critical data and, if so, to triple-check as well as double-check.

Remember that the definition of CI data includes system logs and other administrative data, so this requirement applies to data of that type as well as to data directly used to create V2X messages.

6.3.4.1.43 Storage Integrity for CI Data Entities: Risk Mitigation

For each CI data entity that makes use of stored CI data, the connected intersection shall implement appropriate mechanisms to mitigate the risk that stored data is modified, if this is considered necessary per the evaluation in 6.3.4.1.42.

6.3.4.1.44 List of Privacy-Sensitive Information per CI Data Entity

For each CI data entity, the connected intersection shall maintain an up-to-date list of all privacy-sensitive information that is available for storage or processing by that CI data entity. This includes at least the following if they are available to that CI data entity: privacy-sensitive information that is sent to the CI data entity, privacy-sensitive information that is based on local sensor input, and privacy-sensitive information where multiple inputs that are not individually privacy-sensitive are combined to create information that is privacy-sensitive.

Privacy-sensitive is deliberately not defined here to allow for statutory or other definitions to be applied. The definition used by an individual connected intersection is up to IOO within constraints set by law, regulation, SCMS policy, etc. Note that information about, for example, the location of an RSU is unlikely to be privacy-sensitive. It is most likely that any privacy-sensitive information in the system is information about individual drivers or vehicles.

This requirement covers privacy-sensitive information that resides on a CI data entity, is acted on by a CI data entity, or passes through the CI data entity unprotected. It is not necessary to list any privacy-sensitive information anywhere on the same network as a CI data entity unless there is a defined information flow that transports that privacy-sensitive information to that data entity. In other words, this requirement only needs to be applied to CI data entities that have access by design to that information.

6.3.4.1.45 Protecting Privacy-Sensitive Information per CI Data Entity

For all CI data entities that have access to privacy-sensitive information, the connected intersection shall implement mechanisms to ensure that that information is not improperly accessed while at rest on that component.

This requirement can be fulfilled by ensuring that the access control mechanisms of this section protect access to the privacy-sensitive information.

6.3.4.1.46 CI Data Entity Update: Authorized Sources of CI Software and Firmware

A CI data entity shall implement mechanisms that ensure that all software/firmware updates are obtained from an authorized source.

For example, software/firmware updates received from or recommended by the supplier of the connected intersection could be required to be signed by a code signing key. Software/firmware developed in-house by the CI operator can be assumed to come from an authorized source (assuming that the CI operator has processes in place to prevent unauthorized modification of the software during the development process).

Since software and firmware are CI data, this requirement is implied by other requirements, but it is stated explicitly here for clarity.

6.3.4.1.47 CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates

A CI data entity shall validate the authentication, authorization, and integrity of all software and firmware updates applied to it, including rollbacks to previously installed versions, if supported.

6.3.4.1.48 CI Data Entity Update: Authorized Initiation of Software and Firmware Update

A CI data entity shall implement mechanisms that ensure that all software/firmware updates are initiated as a result of an authorized process that has at some point received the assent of an appropriately authorized user.

This requirement allows automated updates so long as an authorized process has permitted the automated updates to take place.

6.3.4.1.49 CI Data Entity Update: Validation

A CI data entity shall implement mechanisms that ensure that the software/firmware update on a CI data entity is validated before other CI data entities make use of CI data from the updated CI data entity.

This requirement allows automated updates so long as an authorized process has permitted the automated updates to take place.

6.3.4.1.50 CI Data Entity Update: Correct Status

A CI data entity shall implement mechanisms that ensure that it correctly reports software/firmware/configuration version status.

6.3.4.1.51 Protect V2X Radio Parameters

A CI data entity that sends V2X messages shall protect against the V2X radio parameters being modified that cause nonconformance with other requirements.

This can be achieved, for example, by appropriate logical and physical access controls that prevent unauthorized access to those parameters.

6.3.4.1.52 Threat Analysis

A connected intersection shall carry out a threat analysis on each internal CI data entity to identify whether there are threats that might cause incorrect V2X messages to be sent that are not addressed by the requirements above and shall implement mitigations for any non-negligible threats.

6.3.4.2 Data Communications Security

The requirements for data communications security for a connected intersection follow.

6.3.4.2.1 List of Logical Interfaces

A connected intersection shall maintain an up-to-date list of logical interfaces inside the connected intersection and between the connected intersection and external CI data entities, including external V2X message receivers, i.e., all the connections between internal and external CI data entities and all the points where V2X messages are sent by the connected intersection to be received by other road users.

This includes listing all RSUs that send V2X messages. The intent of this requirement is that an agency should maintain an up-to-date list of all RSUs that is maintained by the agency and for each RSU also maintain a list of all messages transmitted by and logical interfaces for each RSU. Without this inventory, an agency could not assess what security gaps may exist.

6.3.4.2.2 Secure Communications for CI Data Logical Interfaces

The connected intersection shall use cryptographic mechanisms to provide integrity and authenticity for all CI data logical interfaces identified in 6.3.4.2.1 except (a) interfaces for which it is identified that it is acceptable to use only physical security and (b) exception cases listed in this document. These are referred to below as "cryptographically protected logical interfaces."

It is up to the connected intersection to determine whether it is acceptable to use only physical security on a particular interface. In general, physical security should be the only source of security if one component is strongly physically secured and has only a single physical connection to another component.

For received V2X messages, this requirement is fulfilled by requiring those messages to have a valid IEEE Std 1609.2 signature. See 6.3.4.4.

EXCEPTION: GNSS data sources are not subject to this requirement.

6.3.4.2.3 Secure Communications: Integrity

The connected intersection shall ensure that for any cryptographically protected CI data logical interface, if an integrity check on a communication across that interface fails, that communication shall be considered in an error state and shall be handled per 6.3.4.2.12.

6.3.4.2.4 Secure Communications: Integrity of External CI Data Outbound Logical Interfaces

The connected intersection shall ensure that for any cryptographically protected CI data logical interface from a component inside the connected intersection to a component outside the connected intersection, a cryptographic integrity check is applied to each communication across that interface and that the external CI data entity has mechanisms in place to mitigate a failure of integrity.

For messages intended to be consumed by vehicles or other road users, i.e., SPaT and MAP messages, this is achieved by IEEE Std 1609.2 signatures. For communications with external data processors, the CI and the external data processor may need to agree on an appropriate integrity mechanism.

6.3.4.2.5 Secure Communications: Replay Protection

For each cryptographically protected CI data logical interface, the connected intersection shall implement replay protection mechanisms across that interface. In other words, the connected intersection shall have a mechanism to ensure that if the same message is retransmitted across the interface, it is not interpreted as two distinct messages to be acted on twice.

This may be a time stamp, a sequence number, or some other mechanism. It may be provided at the communications protocol level (e.g., by IPSec or TLS/SSL) or at the application level.

NOTE: In the specific case of the BSM, which is used by the connected intersection for Assured Green Period (AGP), the signed message includes a time stamp and the BSM can be read as meaning "the sender had the indicated kinematic properties at the indicated time." As such, if a BSM is received twice, the receiver will not treat it as two distinct pieces of information so long as it is written to assume that the important time for the kinematic data is the time in the BSM time stamp rather than the time the BSM is received. In other words, for BSMs, this requirement is fulfilled by writing BSM processing code to use the time in the time stamp rather than the reception time.

6.3.4.2.6 Secure Communications: Plausibility for Received Data

For each CI logical interface, including CI interfaces that are not cryptographically protected, a connected intersection shall identify and implement mechanisms on the receive side to detect whether CI data received over that interface is implausible, i.e., likely to be incorrect (by comparison with other known facts or with previous data received over that interface). If a plausibility check on a communication across that interface fails, that communication shall be considered in an error state and shall be handled per 6.3.4.2.12.

As stated in the requirement, this applies to all CI logical interfaces, including physically protected interfaces and GNSS. In other words, the connected intersection is required to consider GNSS spoofing attacks (but may consider that they are mitigated by protections elsewhere in the system).

NOTE: This is mandatory, but for any given CI logical interface, it is permitted for the connected intersection to fulfill the requirement by identifying that no additional mechanisms are necessary.

6.3.4.2.7 Secure Communications: CI-Internal Logical Component Authentication

The connected intersection shall ensure that for any cryptographically protected CI data logical interface between two components inside the connected intersection, each component authenticates to the other using cryptographic means using credentials that can be used to identify that component as a specific logical functional element inside the connected intersection.

In principle, this requirement could be fulfilled by giving the same credential (and private key) to multiple different physical elements. This is not recommended. If there are multiple physical components that fulfill the same logical functional role, it is instead recommended that each physical component has a different credential and the different credentials are bound to the appropriate logical role; for example, via PSID/SSP if appropriate or via unique component identifiers and a securely distributed access control list (ACL).

"A specific logical functional element" means that the elements must be identified as approved to carry out the specific activities to be carried out over that CI data logical interface, e.g., to be a point of manual entry for MAP message data.

"Failing the authentication check" covers all ways in which the check might fail (e.g., revoked or expired credentials), not just cryptographic failure.

6.3.4.2.8 Secure Communications: CI-Internal Physical Component Authentication

The connected intersection shall ensure that for any cryptographically protected CI data logical interface between two components inside the connected intersection, each component cryptographically authenticates to the other using credentials that can be used to identify that component as a specific physical element inside the connected intersection.

The authentication process of the physical component needs to be tightly bound to any processors where data sourcing, data processing, or message creation takes place; e.g., if there is an HSM that carries out the signing, it should be in the same physically secure housing as any processor that carries out data processing on CI data.

"A specific physical element" means that the elements are identified as particular physical components inside the CI system. The definition of a "particular physical component" can be CI-specific.

"Failing the authentication check" covers all ways in which the check might fail (e.g., revoked or expired credentials), not just cryptographic failure.

NOTE: This is optional because it may not be necessary to identify a particular physical component so long as its functional role is identified.

6.3.4.2.9 Secure Communications: Authentication of External CI Data Logical Interfaces

The connected intersection shall ensure that for any cryptographically protected CI data logical interface from a component outside the connected intersection to a component inside the connected intersection, the external component cryptographically authenticates with a credential that meets a policy set by the connected intersection (or adopted by the connected intersection from a policy developed by some other organization).

"Failing the authentication check" covers all ways in which the check might fail (e.g., revoked or expired credentials), not just cryptographic failure. For example, an IEEE Std 1609.2-signed BSM would fail this check if the certificate is revoked or did not chain back to a known root on a Certificate Trust List (CTL) (or for any other reason for IEEE Std 1609.2 validation to fail).

The policy may be determined by the connected intersection within the constraints of law, regulation, SCMS policy, etc. It should provide assurance that the credential issuer has taken care to ensure that the credential holder is entitled to the credential. The credential issuer may have a policy for credential issuance that is appropriate for the needs of the connected intersection. In this case, that existing policy (so long as it has been reviewed to make sure it does in fact satisfy the needs of the connected intersection) fulfills this requirement.

6.3.4.2.10 Secure Communications: Authentication of External CI Data Outbound Logical Interfaces

The connected intersection shall ensure that for any cryptographically protected CI data logical interface from a component inside the connected intersection to a component outside the connected intersection, a cryptographic authentication mechanism is applied to each communication across that interface.

For messages intended to be consumed by vehicles or other road users, this is achieved by IEEE Std 1609.2 signatures. For communications with external data processors, the connected intersection and the external data processor may need to agree to an appropriate authentication mechanism.

6.3.4.2.11 Secure Communications: Check Authentication for Received Data

For each cryptographically protected CI data logical interface, a CI data component shall check the authentication of inbound CI data communications. If an authentication check on a communication across that interface fails, that communication is considered to be in an error state and is handled per 6.3.4.2.12.

NOTE: This requirement covers all aspects of checking the authentication for received data, including checking the validity of credentials associated with received data, which in turn includes checking that already trusted credentials have not expired or been revoked.

6.3.4.2.12 Secure Communications: Manage Received Data for Which Checks Have Failed

For each CI data logical interface, a connected intersection shall have a policy for how the receiver reacts if any of the above checks fail (if applicable) on received CI data. The policy should require the receiver to do one or more of (a) attempt to recover automatically, i.e., to produce valid output without using the suspect data; (b) notify the CPMS which will manage a central response such as notifying an operator; (c) directly notify an operator; (d) locally log the failure; (e) stop sending V2X messages or other CI data; and/or (f) inform receivers of that CI data that the data is not available or suspect. Additional mitigations may also be implemented.

The "if applicable" above is because some checks apply only to cryptographically protected data while others apply to all data.

The reaction may depend on the type of data and on the type of the failure, i.e., different types of data and/or different types of failure can lead to different reactions.

6.3.4.2.13 Secure Communications: External Data Entities for Which Checks Have Failed

For each CI data logical interface, the connected intersection shall have a policy as to whether and under what circumstances the operator of an external CI data entity is notified of failures of applicable checks for inbound communications from that data entity across that interface.

The connected intersection might not have a business relationship with the operator of the external data entity by which it can directly inform that operator of issues. But there might be online forums or other means by which the connected intersection can inform the operator.

If a sender fails an authentication or integrity check, it is possible that the incoming communication is spoofed by a third party and so is not under the control of the sender. In this case, the sender might not be able to do anything to resolve the issue. This does not necessarily affect whether the CI operator should inform an external CI data entity of an authentication failure, but the CI operator should have reasonable expectations about what the external entity can do.

NOTE: It is mandatory to have a policy on when to inform; it is not mandatory to inform.

6.3.4.2.14 Secure Communications: Other Users of External Data Entities for Which Checks Have Failed

For each CI data logical interface, the connected intersection shall have a policy as to when to attempt to inform other users of an external CI data entity if there is a failure of applicable checks for inbound communications from that data entity across that interface.

NOTE: It is mandatory to have a policy on when to inform; it is not mandatory to inform. It might be hard to find other users, although there might be online customer forums or other kinds of information exchange set up as an external service. The policy doesn't have to be specific and reporting can be at the discretion of individuals, but it is recommended that if there is a significant failure (for some definition of significant) on inbound data from an external CI data entity, then the connected intersection makes reasonable efforts to make sure this is known to other users of the data who may experience bad outcomes from its use.

6.3.4.2.15 Entitlement to Authentication Credentials

For each cryptographically protected CI data logical interface, the connected intersection shall have a policy as to what conditions need to be met for credentials to be issued to the components on either side of the interface such that the policy gives assurance that the components fulfill the requirements appropriate for the actions carried out by those components. These requirements are to include the data source and processing requirements above where appropriate.

The policy is to identify the cybersecurity and functional requirements to be fulfilled by the CI data entity; how the credential issuer determines those requirements have been fulfilled; and how the credential issuer determines that the CI data entity is entitled to assert any other information contained in the credentials, such as role, identity, permissions, location, etc.

The policy may be determined by the connected intersection within the constraints of law, regulation, SCMS policy, etc. It should provide assurance that the credential issuer has taken care to ensure that the credential holder is entitled to the credential. The credential issuer may already have a policy for credential issuance that is appropriate for the needs of the connected intersection. In this case, that existing policy (so long as it has been reviewed to make sure it does in fact satisfy the needs of the connected intersection) fulfills this requirement.

For example, SCMS providers are already establishing IEEE Std 1609.2 certificate issuance policies for BSM senders.

6.3.4.2.16 Secure Issuance of Authentication Credentials

For each component in the connected intersection that receives an authentication credential, the connected intersection shall implement a secure provisioning mechanism for those credentials that provides integrity protection and mutual authentication of the component to the credential provider.

NOTE: For IEEE Std 1609.2 certificates, this requirement is fulfilled by using the CAMP protocols or IEEE Std 1609.2.1.

6.3.4.2.17 Secure Re-Issuance of Authentication Credentials

For each component in the connected intersection that receives an authentication credential, that credential shall have a known expiry date, and the connected intersection shall implement, in coordination with the credential provider, a process to ensure secure re-provisioning in a timely manner before the expiry time of the current credential.

For IEEE Std 1609.2 certificates, this requirement is fulfilled by using the CAMP protocols or IEEE Std 1609.2.1.

NOTE: In the above requirement, "timely" is deliberately not precisely defined. The definition used by an individual connected intersection may be specific to that connected intersection within constraints set by law, regulation, SCMS policy, etc. For further discussion, see the design section.

6.3.4.2.18 Blocking Re-Issuance of Authentication Credentials

For each component in the connected intersection that receives an authentication credential, the connected intersection shall implement, in coordination with the credential provider, a process to notify the credential provider before the succeeding credential is issued if the component is no longer entitled to a credential.

For IEEE Std 1609.2 certificates signing SPaT or MAP messages, there may be misbehavior reporting implemented on the receiver side (i.e., on the vehicles) that leads to the credentials not being reissued even without the connected intersection notifying the SCMS. However, the main focus of this requirement is that there needs to be a way for the connected intersection to notify the SCMS if, for example, a component has been taken out of service and should no longer be issued credentials.

6.3.4.2.19 List of Privacy-Sensitive Information Flows

A connected intersection shall maintain an up-to-date list of all information flows that result in a component inside the connected intersection obtaining, creating, or sending privacy-sensitive information.

NOTE: As discussed in 6.3.4.1.44, "privacy-sensitive" is deliberately not defined here to allow for statutory or other definitions to be applied. Privacy-sensitive information can be created on a component when multiple inputs that are not individually privacy-sensitive are combined to create information that is privacy-sensitive; in other words, an information flow can result in a component having privacy-sensitive information even if the information in the flow is not itself privacy-sensitive.

6.3.4.2.20 Protecting Privacy-Sensitive Information Flows

For all information flows that result in a component inside the connected intersection obtaining, creating, or sending privacy-sensitive information, the connected intersection shall use mechanisms to protect against that information being accessed while in transit.

In general, this can be done by encryption. For received BSMs, the privacy mechanisms applied by the BSM sender can be considered sufficient to fulfill this requirement.

NOTE: For clarity, this does not apply to GNSS signals, as GNSS signals do not become privacy-sensitive until they are processed by a receiver using receiver-specific information (i.e., time of arrival) and become positioning information. Positioning information obtained from the processing of GNSS signals can, however, be privacy-sensitive and should be considered in a privacy analysis.

6.3.4.2.21 Protecting Sent Privacy-Sensitive Information when Received

For all information flows in which a component inside the connected intersection sends privacy-sensitive information to a component outside the connected intersection, the connected intersection shall require that the receiver has a policy for management of privacy-sensitive information that protects that information from being improperly accessed either by the initial receiver or by downstream receivers.

NOTE: Broadcast MAP, SPaT, and RTCMcorrections messages are not considered privacy-sensitive information and so the connected intersection does not need to ensure that receivers protect them.

6.3.4.2.22 Security Size Overhead

The cryptographic security mechanisms applied to cryptographically protected CI logical interfaces shall not create message size overhead that conflicts with CTI 4501, 6.3.3.1.3.1, Transport Message Size - WAVE.

For V2X messages, this is fulfilled by the use of IEEE Std 1609.2 signing.

6.3.4.2.23 Security Processing Overhead

The cryptographic security mechanisms applied to cryptographically protected CI logical interfaces shall not create message processing overhead that conflicts with CTI 4501, 6.3.3.1.5, Timeliness Requirements.

For V2X messages, this is fulfilled by the use of IEEE Std 1609.2 signing and verification.

6.3.4.2.24 Protection of Cryptographic Keying Material: General

For each CI data entity that authenticates itself over a cryptographically protected CI logical interface, the connected intersection shall analyze the impact of exposure of the cryptographic keys used for source authentication, i.e., the CI shall evaluate what damage is potentially done to the correct operation of the system if that CI data entity's authentication keys become known to a malicious party.

6.3.4.2.25 Protection of Cryptographic Keying Material: Hardware

For each CI data entity that authenticates itself over a cryptographically protected CI logical interface, the cryptographic keys used for source authentication shall be protected from exposure by the use of cryptographic hardware, where the level of hardware protection is appropriate to the impact of compromise of the keys and the ease of physical access to the CI data entity.

NOTE: The use of NIST FIPS 140-2 compliant HSMs will in general fulfill this requirement, but connected intersections may also determine that due to restrictions on physical access to certain CI data entities, it is not necessary to have dedicated cryptographic hardware on those CI data entities.

6.3.4.2.26 Protection of Cryptographic Keying Material: Access to and Use of Keys

For each CI data entity that authenticates itself over a cryptographically protected CI logical interface, the cryptographic keys used for source authentication shall be protected from uses other than the intended and authorized uses.

This means that, for example, if an RSU signs SPaT messages, it can't be tricked into signing something else with the SPaT signing keys - in other words, an attacker can't create a fake SPaT and submit it for signing.

To demonstrate that this requirement is fulfilled, a connected intersection will need to show what restrictions are in place that prevent an unintended process on the CI data entity from requesting use of the authentication key and what restrictions are in place to ensure that an intended process only submits correct inputs to the authentication generation process.

6.3.4.3 Trustworthiness of TSC-Originating Information

The requirements for trustworthiness of TSC-originating information for a connected intersection follow.

6.3.4.3.1 TSC Infrastructure Protection: Invalid Signal Timing Information

A TSC infrastructure shall be protected against modification that would make it send invalid or incorrect signal timing data or status.

6.3.4.3.2 TSC Infrastructure Protection: Invalid Format for Signal Timing Information

A TSC infrastructure shall be protected against modification that would make it send signal timing data or status represented in a format other than the valid SPaT information formats specified in CTI 4501/1, 6.3.2.1, TSC Infrastructure Signal Timing Data Requirements.

6.3.4.3.3 TSC Infrastructure Protection: Incorrect Format for Signal Timing Information

A TSC infrastructure shall be protected against modification that would make it send a SPaT information in a particular valid format specified in CTI 4501/1, 6.3.2.1, TSC Infrastructure Signal Timing Data Requirements, when the RSU is expecting a SPaT information in a different valid format.

6.3.4.3.4 TSC Infrastructure Protection: Invalid Contents for Signal Timing Data

A TSC infrastructure shall be protected against modification that would cause SPaT information not to be conformant with the requirements of CTI 4501/1, 6.3.2.1.1.1, 6.3.2.1.1.2, 6.3.2.1.1.3, 6.3.2.2, 6.3.3.1.2.1, 6.3.3.1.6.1, and 6.3.3.1.6.3.

In addition to these security requirements for SPaT information, there are additional requirements identified in 6.3.4.7 for creating the encoded SPaT message. If the TSC infrastructure creates the encoded SPaT message, those requirements will also apply to the TSC infrastructure.

6.3.4.3.5 Information About Availability of SPaT Information

A connected intersection shall implement mechanisms to prevent the RSU incorrectly believing that the TSC infrastructure is not providing (or providing invalid) signal timing data or status.

6.3.4.4 Approaching Vehicle Information Trustworthiness: RSU

The security requirements for RSU approaching vehicle information trustworthiness for a connected intersection follow.

6.3.4.4.1 Validate Security of Approaching Vehicle V2X Messages

An RSU shall check that received V2X messages about vehicle dynamics meet appropriate communications security validation conditions before making use of those messages.

In practice, the messages are BSMs and the appropriate communications security validation condition is to check that they are validly signed per IEEE Std 1609.2.

NOTE: This does not create a requirement for the RSU to validate the contents of the message, only the security envelope.

6.3.4.4.2 Validate Approaching Vehicle V2X Messages: Replay

An RSU shall ensure that if the same information about an approaching vehicle is provided twice, it is not considered to be information about two distinct vehicles.

The IEEE Std 1609.2 security profile for BSM leaves this determination to the application, i.e., the IEEE Std 1609.2 security services are not responsible for checking for replayed BSMs.

6.3.4.4.3 Validate Approaching Vehicle V2X Messages: Misbehavior Detection

An RSU shall apply appropriate misbehavior detection mechanisms to received V2X messages. Misbehavior mechanisms are defined in SAE J3287. An RSU may also apply additional misbehavior detection mechanisms such as detecting malformed received BSMs, or BSM-like messages with a non-BSM PSID, or messages that failed IEEE Std 1609.2 validation.

NOTE: This requirement is optional because the CI operator may determine that existing misbehavior detection mechanisms are not worth the cost of implementing and running them. It is possible that external conditions such as SCMS policy require misbehavior detection to be implemented even though this requirement is optional in CTI 4501.

6.3.4.4.4 Validate Approaching Vehicle V2X Messages: Misbehavior Reporting

An RSU shall report received V2X messages that are determined to be misbehavior. Misbehavior reporting mechanisms are defined in SAE J3287.

NOTE: This requirement is optional because the CI operator may determine that existing misbehavior reporting mechanisms are not worth the cost of implementing and running them. It is possible that external conditions such as SCMS policy require misbehavior reporting to be implemented even though this requirement is optional in this document.

6.3.4.4.5 Validate Approaching Vehicle V2X Messages: Distinguish Between Senders

A connected intersection shall have a capability to determine whether different trust levels should be associated with different BSM senders or groups of BSM senders. The RSU is to apply these different trust levels if appropriate in the validation of those messages.

Examples of how BSM senders could be distinguished include: by their issuing Certificate Authority (CA); by their root CA; by an OperatingOrganizationId if that appears in their IEEE Std 1609.2 certificate; or by whether they are identified or pseudonym certificates.

NOTE 1: The BSM filtering feature of an RSU is defined in 3.3.2.9.2.1 and 4.3.2.14.4 of CTI 4001. Requirements in this section may be duplicative of requirements in CTI 4001 and are included here for completeness.

NOTE 2: This is an optional requirement and there is no expectation that it is implemented.

6.3.4.4.6 Security for Use of RSU BSM Filtering for RDZ

An RSU that is intended to use BSM filtering for RDZ shall be protected against being configured not to use BSM filtering.

6.3.4.4.7 Security for Configuration of RSU BSM Filtering for RDZ

An RSU that is intended to use BSM filtering for RDZ shall be protected against being configured with incorrect RDZ definitions.

6.3.4.5 Approaching Vehicle Information Trustworthiness and AGP: TSC

The security requirements for TSC approaching vehicle information trustworthiness and AGP for a connected intersection follow.

NOTE: The TSC infrastructure is a CI data entity. As such, the TSC infrastructure is subject to the requirements of 6.3.4.1, and communications with the TSC infrastructure are subject to the requirements of 6.3.4.2.

6.3.4.5.1 Protection from Unnecessary AGP

A TSC infrastructure shall be protected so that it does not initiate an AGP other than when it believes a V2X-equipped vehicle is approaching in an AGP-causing state.

6.3.4.6 Time Source Trustworthiness

The requirements for time source trustworthiness and AGP for a connected intersection follow.

NOTE: If the time source is a GNSS time source, it is exempt from some of the communications security requirements of 6.3.4.2 as discussed in the definition of "CI data communications." Otherwise, the time source is a CI data entity and, as such, the time source is subject to the requirements of 6.3.4.1, and communications with the time source are subject to the requirements of 6.3.4.2.

6.3.4.6.1 Availability of Time Sources

A connected intersection shall analyze whether information from time sources can potentially be delayed and whether this delay can lead to the connected intersection having an understanding of time that is not consistent with CTI 4501, 6.3.3.2.1, Time Accuracy.

6.3.4.6.2 Detect Time Source Delay

If time source delay is possible and can lead to the connected intersection having an understanding of time that is not consistent with CTI 4501, 6.3.3.2.1, Time Accuracy, then the connected intersection shall implement mechanisms to detect whether time source delay is happening.

6.3.4.6.3 Manage Time Source Delay

A connected intersection shall have a policy for how the receiver reacts if time source delay is detected. The policy shall require the receiver to do one or more of: (a) attempt to recover automatically, i.e., to produce valid output without using the delayed time; (b) notify the CPMS, which will manage a central response such as notifying an operator; (c) directly notify an operator; (d) locally log the failure; and/or (e) stop sending V2X messages or other CI data and, optionally, inform receivers of that information that the information is not available. Additional mitigations may also be implemented.

6.3.4.6.4 Time Source Delay for External Time Sources

A connected intersection shall have a policy as to whether and under what circumstances the operator of an external time source is notified of detected time source delay.

The connected intersection might not have a business relationship with the operator of the external data entity by which it can directly inform that operator if issued. But there might be online forums or other means by which the connected intersection can inform the operator.

NOTE: It is mandatory to have a policy on when to inform; it is not mandatory to inform.

6.3.4.6.5 Time Source Delay for External Time Sources: Other Users

A connected intersection shall have a policy as to whether and under what circumstances other users of an external time source is notified of detected time source delay. See discussion in 6.3.4.2.14 of how other users could be informed.

NOTE: It is mandatory to have a policy on when to inform; it is not mandatory to inform.

6.3.4.7 SPaT Message Trustworthiness and Reliability

The requirements for SPaT message trustworthiness and reliability for a connected intersection follow.

This section contains requirements that apply to all SPaT message elements identified in CTI 4501. Some message elements have additional, specific requirements, which are listed later. This section also assumes that SPaT messages are always generated inside the connected intersection.

6.3.4.7.1 List of CI Data Entities that Affect SPaT Contents

The connected intersection shall maintain an up-to-date list of all CI data entities that produce or store data that affects SPaT production, or that encode SPaT messages, or that have write access to encoded SPaT messages before they are signed. These are referred to as "SPaT-impacting CI data entities" below.

All entities that affect the contents of SPaT messages are CI data entities and so are subject to the requirements of 6.3.4.1, including the requirement to note which CI data entities are used for manual data entry. If there are CI data entities on which data that affects SPaT messages is entered manually, those CI data entities are subject to the requirements of 6.3.4.1.4 and 6.3.4.1.23.

All external SPaT-impacting CI data entities are subject to the specific requirements in 6.3.4.1 for external CI data entities.

All communications between SPaT-impacting CI data entities are communications between CI data entities and so are subject to the requirements of 6.3.4.2 (with exceptions, as noted inline in those requirements, for GNSS data sources).

6.3.4.7.2 Prevent Invalid SPaT Contents or Behavior

The connected intersection shall implement mechanisms to protect any internal SPaT-impacting CI data entities against modification that would cause SPaT messages or SPaT transmission behavior not to be conformant with the requirements of CTI 4501/1, 6.3.3.2.2.1, 6.3.3.2.2.2, 6.3.3.2.3.1, 6.3.3.2.3.2, 6.3.3.3.1, 6.3.3.3.2, 6.3.3.3.3, 6.3.3.3.4, 6.3.3.3.5, 6.3.3.3.6.1, 6.3.3.3.7, 6.3.3.3.8, and 6.3.3.4.7 (if those requirements are applicable for the particular connected intersection).

6.3.4.7.3 Detect Inconsistency of SPaT and Signal Timing Data

A connected intersection shall have mechanisms to detect (or otherwise be informed) in a timely manner if the generated SPaT message signal timing data or status becomes inconsistent with the signal timing data or status provided to the RSU and/or the physical signal indications.

This can be fulfilled by a number of means, including: setting up system monitoring with cameras; providing a phone number that people can call if the SPaT is mismatched (and the phone number can be provided either via signage or within a V2X message); or misbehavior detection, i.e., autonomous misbehavior detection carried out by approaching vehicles and reported to an appropriate authority.

NOTE: In the above requirement, "timely" is deliberately not precisely defined. The definition used by an individual connected intersection may be specific to that connected intersection within constraints set by law, regulation, SCMS policy, etc. For further discussion, see the design section.

6.3.4.7.4 Manage Inconsistency of SPaT and Signal Timing Data

A connected intersection shall have a policy for action to take if inconsistency is detected between the generated SPaT message and the signal timing data or status provided to the RSU and/or the physical signal indications. The action(s) to take shall include at least one of: (a) attempt to recover automatically, i.e., to automatically bring the SPaT in conformance with the behavior and validate that that has occurred; (b) notify the CPMS, which will manage a central response such as notifying an operator; (c) directly notify an operator; (d) locally log the failure; and/or (e) stop sending V2X messages or other CI data and, optionally, inform receivers of that information that the information is not available. Additional mitigations may also be implemented.

6.3.4.8 MAP Message Contents Trustworthiness

The requirements for MAP message contents trustworthiness for a connected intersection follow.

NOTE: This section contains requirements that apply to all MAP message elements identified in CTI 4501. Some message elements have additional, specific requirements, which are listed later.

6.3.4.8.1 List of CI Data Entities that Affect MAP Contents

The connected intersection shall maintain an up-to-date list of all CI data entities that produce or store data that affects MAP production, or that encode MAP messages, or that have write access to encoded MAP messages before they are signed. These are referred to as "MAP-impacting CI data entities" below.

All entities that affect the contents of MAP messages are CI data entities and so are subject to the requirements of 6.3.4.1, including the requirement to note which CI data entities are used for manual data entry. If there are CI data entities on which data that affects MAPs is entered manually, those CI data entities are subject to the requirements of 6.3.4.1.4 and 6.3.4.1.23. (For MAPs, there may be a significant number of potential manual data entry points, especially compared to SPaTs, so the manual data entry security requirements may be particularly significant for MAP.) All external MAP-impacting CI data entities are subject to the specific requirements in 6.3.4.1 for external CI data entities. All communications between MAP-impacting CI data entities are communications between CI data entities and so are subject to the requirements of 6.3.4.2 (with exceptions, as noted inline in those requirements, for GNSS data sources).

6.3.4.8.2 Prevent Invalid MAP Contents or Behavior

The connected intersection shall implement mechanisms to protect any internal MAP-impacting CI data entities against modification that would cause MAP messages or transmission behavior not to be conformant with the requirements of CTI 4501/2, 6.3.3.2.2.3, 6.3.3.2.2.4, 6.3.3.2.2.5, 6.3.3.2.2.6, 6.3.3.4.1, 6.3.3.4.2, 6.3.3.4.3, 6.3.3.4.4, 6.3.3.4.5, and 6.3.3.4.6 and CTI 4501/1, 6.3.3.4.7 (if those requirements are applicable for the particular connected intersection).

The external CI data entities are to be listed on the list required by 6.3.4.8.1.

Requirements on external CI data entities are given in some of the 6.3.4.1 requirements. Requirements on communications with external CI data entities are given in 6.3.4.2.

NOTE: This requirement is conditionally mandatory because it applies only to the case where a connected intersection has the MAP generated inside the connected intersection. A connected intersection may also have the MAP message generated outside the connected intersection, in which case 6.3.4.8.3 applies instead.

6.3.4.8.3 External MAP Message Generation or Partial Generation: Data Source

If a MAP message is generated outside the connected intersection or is constructed using data obtained from a source or processor outside the connected intersection, the data source or processor shall be treated as an external CI data entity and shall be subject to the relevant requirements of 6.3.4.1.

NOTE: This is conditionally mandatory because it applies only to the case where a connected intersection has the MAP or some MAP data generated outside the connected intersection. A connected intersection may also have the MAP message and all of the relevant input data generated inside the connected intersection, in which case 6.3.4.8.2 applies instead. (It seems very likely that this requirement will apply in many cases, e.g., if external surveyors are used.)

6.3.4.8.4 Prevent Inconsistency of MAP and Road Geometry or Use: False Positives

A connected intersection shall have mechanisms to prevent a malicious actor from causing a modified MAP to be sent from CI equipment when the intersection geometry or use has not changed.

This covers use cases that are covered by the data entry and data source requirements above but also covers the case where, for example, an attacker causes an old MAP to be sent in such a way that it will be treated as current by receivers.

6.3.4.8.5 Prevent Inconsistency of MAP and Road Geometry or Use: False Negatives

A connected intersection shall have mechanisms to prevent a malicious actor from causing a modified MAP NOT to be sent from CI equipment when the intersection geometry or use HAS changed.

NOTE: The upper-case "NOT" and "HAS" are to highlight the contrast with 6.3.4.8.4.

6.3.4.8.6 Detect Inconsistency of MAP and Road Geometry or Use

A connected intersection shall have mechanisms to detect (or otherwise be informed) in a timely manner if the generated MAP message is inconsistent with the road geometry or other attributes.

This can be fulfilled by a number of means, including setting up system monitoring with cameras; providing a phone number that people can call if the MAP is mismatched (and the phone number can be provided either via signage or within a V2X message); and misbehavior detection, i.e., autonomous misbehavior detection carried out by approaching vehicles and reported to an appropriate authority.

NOTE: In the above requirement, "timely" is deliberately not precisely defined. The definition used by an individual connected intersection may be specific to that connected intersection within constraints set by law, regulation, SCMS policy, etc. For further discussion, see the design section.

6.3.4.8.7 Manage Inconsistency of MAP and Road Geometry or Use

A connected intersection shall have mechanisms to manage inconsistency of the generated MAP message and the road geometry or other attributes. The policy shall require the connected intersection to do one or more of: (a) attempt to recover automatically (if this is possible); (b) notify the CPMS, which will manage a central response such as notifying an operator; (c) notify an operator; (d) locally log the failure; and/or (e) stop sending V2X messages or other CI data and, optionally, inform receivers of that information that the information is not available. Additional mitigations may also be implemented.

6.3.4.9 RTCM Message Contents Trustworthiness

The requirements for RTCM message contents trustworthiness for a connected intersection follow.

NOTE: This section contains requirements that apply to all RTCM message elements identified in CTI 4501. Some message elements have additional, specific requirements, which are listed later.

6.3.4.9.1 List of CI Data Entities that Affect RTCM Contents

The connected intersection shall maintain an up-to-date list of all CI data entities that produce or store data that affects RTCM production, or that encode RTCM messages, or that have write access to encoded RTCM messages before they are signed. These are referred to as "RTCM-impacting CI data entities" below.

All entities that affect the contents of RTCM messages are CI data entities and so are subject to the requirements of 6.3.4.1, including the requirement to note which CI data entities are used for manual data entry. If there are CI data entities on which data that affects RTCM is entered manually, those CI data entities are subject to the requirements of 6.3.4.1.4 and 6.3.4.1.23. All external RTCM-impacting CI data entities are subject to the specific requirements in 6.3.4.1 for external CI data entities. All communications between RTCM-impacting CI data entities are communications between CI data entities and so are subject to the requirements of 6.3.4.2 (with exceptions, as noted inline in those requirements, for GNSS data sources).

6.3.4.9.2 Prevent Invalid RTCM Contents or Behavior

The connected intersection shall implement mechanisms to protect any internal RTCM-impacting CI data entities against modification that would cause RTCM messages or behavior not to be conformant with the requirements of SAE J3258, 6.3.1.

6.3.4.9.3 External RTCM Message Generation or Partial Generation: Data Source

If an RTCM message is generated outside the connected intersection or is constructed using data obtained from a source or processor outside the connected intersection, the data source or processor shall be treated as external CI data entity and subject to the relevant requirements of 6.3.4.1.

NOTE: This is conditionally mandatory because it applies only to the case where a connected intersection has the RTCM or some RTCM data generated outside the connected intersection. A connected intersection may also have the RTCM message and all of the relevant input data generated inside the connected intersection, in which case 6.3.4.9.2 applies instead.

6.3.4.10 Consistency Between MAP and SPaT Messages

The security requirements for consistency between MAP and SPaT messages for a connected intersection follow.

6.3.4.10.1 SPaT and MAP Version Consistency

The connected intersection shall implement mechanisms such that the processes inside the connected intersection that provide assurance that SPaT and MAP content versions are consistent and protected against malicious modification.

6.3.4.10.2 SPaT and MAP Intersection Identifier Consistency

The connected intersection shall implement mechanisms such that the processes inside the connected intersection that provide assurance that SPaT and MAP use the same intersection identifiers are protected against malicious modification.

6.3.4.11 Unavailability Indications

The requirements for unavailability indications for a connected intersection follow.

6.3.4.11.1 Correctness of SPaT Availability Indications

The connected intersection shall implement mechanisms to ensure that a SPaT is not indicated as available in a message when it is not available.

6.3.4.11.2 Correctness of SPaT Unavailability Indications

The connected intersection shall implement mechanisms to ensure that a SPaT is not indicated as unavailable in a message when it is available.

6.3.4.11.3 Correctness of MAP Availability Indications

The connected intersection shall implement mechanisms to ensure that a MAP is not indicated as available in a message when it is not available.

6.3.4.11.4 Correctness of MAP Unavailability Indications

The connected intersection shall implement mechanisms to ensure that a MAP is not indicated as unavailable in a message when it is available.

6.3.4.11.5 Correctness of RTCM Availability Indications

The connected intersection shall implement mechanisms to ensure that an RTCM is not indicated as available in a message when it is not available.

6.3.4.11.6 Correctness of RTCM Unavailability Indications

The connected intersection shall implement mechanisms to ensure that an RTCM is not indicated as unavailable in a message when it is available.

6.3.4.12 Intersection Identifier Trustworthiness

The requirements for intersection identifier trustworthiness for a connected intersection follow.

All sources of intersection identifiers will be an authorized and authenticated CI data entity subject to the requirements of 6.3.4.1, and the communications from the identifier source to the location where the identifier is used will be cryptographically protected. Specific additional requirements for identifier sources and for identifiers follow.

6.3.4.12.1 Robustness of Intersection Identifier Assignment

The connected intersection shall document how intersection identifiers are assigned, including how it mitigates the risk that the same identifier is assigned to more than one intersection.

6.3.4.12.2 Detect Incorrect Intersection Identifiers

A connected intersection shall have mechanisms to detect (or otherwise be informed) in a timely manner if a SPaT or a MAP message that is intended to refer to a particular intersection within the connected intersection uses an identifier other than the one assigned to that intersection.

This includes detecting duplicate identifiers, because if two different intersections are using the same identifier, then at least one of them is using the one not assigned to it. Since this requirement is optional, a connected intersection may choose to partially fulfill it by implementing only duplicate detection rather than detection of all incorrect IDs on the grounds that incorrect assignment of a valid identifier to a second intersection is the most likely failure mode and easy to detect (and can be detected without providing the detection units with the correct list of IDs, which by assumption might itself be wrong).

The most natural way to do this: The connected intersection will already have processes in place to check on the ground that output is correct, for example, by having mobile units that compare V2X message output to local observations. These processes include knowledge of the correct ID for an intersection at a particular location. Whenever an intersection is checked, the checking process includes a check that the correct ID is being used.

NOTE 1: In the above requirement, "timely" is deliberately not precisely defined. The definition used by an individual connected intersection may be specific to that connected intersection within constraints set by law, regulation, SCMS policy, etc. For further discussion, see the design section.

NOTE 2: This is optional because if the assignment process is sufficiently robust, then the risk of using an incorrect identifier is very low, and there is no benefit to implementing the detection mechanisms as there will be nothing to detect.

6.3.4.12.3 Manage Incorrect Intersection Identifiers

If a SPaT or MAP message that is intended to refer to a particular intersection within the connected intersection is detected to be using an identifier other than the one assigned to that intersection, the detection/diagnostic system shall do one or more of: (a) attempt to recover automatically, i.e., to correct the intersection identifier in the systems that are producing the messages with the incorrect identifier; (b) notify the CPMS, which will manage a central response such as notifying an operator; (c) directly notify an operator; (d) locally log the failure; or (e) stop sending V2X messages or other CI data and, optionally, inform receivers of that information that the information is not available. Additional mitigations may also be implemented.

NOTE: This is optional because if the assignment process is sufficiently robust, then the risk of this situation arising is very low.

6.3.4.12.4 Detect Duplicate Use of Intersection Identifiers by External Parties

A connected intersection shall have mechanisms to detect (or otherwise be informed) in a timely manner if an intersection not under its control incorrectly uses an identifier assigned to an intersection not under its control (or uses any identifier within the set of identifiers intended to be associated with the subject connected intersection even if it is not currently in use).

NOTE 1: In the above requirement, "timely" is deliberately not precisely defined. The definition used by an individual connected intersection may be specific to that connected intersection within constraints set by law, regulation, SCMS policy, etc. For further discussion, see the design section.

NOTE 2: This is optional because it’s very unlikely to happen, it’s not clear how it could be detected, it’s not clear what to do about it, and the impact of having two geographically distant intersections use the same identifier seems low.

6.3.4.12.5 Manage Duplicate Use of Intersection Identifiers by External Parties

A connected intersection shall have mechanisms to manage the case where an intersection not under its control incorrectly uses an identifier assigned to an intersection not under its control (or uses any identifier within the set of identifiers intended to be associated with the subject CI even if it is not currently in use).

Examples of appropriate mechanisms: inform the operator of the external intersection; inform the SCMS or other credential management service; and inform some other authority. Further detail is provided in the design section.

NOTE: This is optional because it’s very unlikely to happen, it’s not clear how it could be detected, it’s not clear what to do about it, and the impact of having two geographically distant intersections use the same identifier seems low.

6.3.4.13 System Management and Recovery

The requirements for system management and recovery for a connected intersection follow.

6.3.4.13.1 System Recovery - Software and Configuration Backups

A connected intersection shall maintain system software and configuration backups that are integrity protected and maintained separately from the connected intersection.

6.3.4.13.2 List of Operator-Notifiable Events

The connected intersection shall identify system monitoring events (or types of events) for the system monitoring function that will notify a human operator.

6.3.4.13.3 List of Systemic Failure Events

The connected intersection shall have a list of systemic failure events for which a recovery plan is specified (for example, due to cyberattacks, power outages, physical events).

The plan may, but does not have to, depend on the error state in question.

6.3.4.13.4 Cyberattack Must be Addressed

The list specified in 6.3.4.13.2 shall include cyberattacks as a systemic failure event to be considered.

6.3.4.13.5 Recovery Plan from Systemic Failure

For each systemic failure event in the list, the connected intersection shall have a plan to recover from that event and to validate such recovery for the system. The plan may, but does not have to, depend on the error state in question. The recovery process may include stopping sending V2X messages or other CI data until the issue is resolved.

This requirement is in addition to the recovery plans for individual components specified in 6.3.4.1.31.

6.3.4.13.6 Recovery from Systemic Failure Only When Necessary

The connected intersection shall have mechanisms to prevent a recovery plan from a systemic failure event from being triggered when it is not necessary.

The plan may, but does not have to, depend on the error state in question.

NOTE: This requirement is in addition to the recovery plans for individual components specified in 6.3.4.1.31.

6.3.4.13.7 Preserve Access Control During Systemic Failure

The recovery plan for a systemic failure event shall maintain a reasonable level of physical and logical access security for CI data entities during the event.

It is not anticipated that all access controls can be maintained under all circumstances; for example, if someone drives a truck into a secure building. The intent of this requirement is to have the connected intersection implement mechanisms that will be effective under a range of reasonable error states.

NOTE: In the above requirement, "reasonable" is deliberately not precisely defined. The definition is left to the IOO's discretion within bounds set by law, regulation, SCMS policy, etc. This may include changing the privileges granted to specific personnel, or personnel in specific roles or job titles, based on the error state. For example, an employee may have a key to a locked room that they are allowed to use only in the event of a power outage.

6.3.4.13.8 Robustness of Recovery from Systemic Failure

A connected intersection shall implement mechanisms to protect against disruption, malicious or otherwise, of recovery from systemic failure.

6.3.4.13.9 Assurance of Recovery from Systemic Failure

A connected intersection shall implement mechanisms to provide assurance that the recovery state relative to systemic failure is not reported incorrectly (recovered when not recovered or not recovered when recovered).

6.3.4.13.10 Source Assurance for Recovery from Failure for Internal Data Sources or Processors

A connected intersection shall implement mechanisms to provide assurance that information about the recovery state relative to system-wide or distributed errors is accepted only from authorized sources.

6.3.4.13.11 Automated Recovery from Failure for the CI is not to be an Attack Vector

For each mechanism for automated recovery from an error state within the connected intersection, the connected intersection shall analyze the risk that the automated recovery mechanism can be maliciously misused and mitigate any identified significant risks.

NOTE: In the above requirement, "significant" is deliberately not precisely defined. The definition used by an individual CI may be specific to that CI within constraints set by law, regulation, SCMS policy, etc. For further discussion, see the design section.

6.3.4.13.12 Vulnerability Management for Potential Cyberattack

A connected intersection shall have a process to be informed of potential vulnerabilities in CI data entities, to determine whether the potential vulnerabilities lead to risks, to evaluate the risks, and to address significant risks.

For example, the connected intersection could subscribe to vulnerability disclosure bulletins and scan them for vulnerabilities affecting CI data entities inside the connected intersection; or the connected intersection could require that suppliers have a program to discover vulnerabilities (by internal research or by scanning bulletins) and disclose those vulnerabilities to customers; or a combination of the two; or some other approach.

Newly identified risks could be addressed in many ways, for example, by updating affected CI data entities, by adding material specific to the new risk to the recovery plan, or by reviewing the existing recovery plan and determining that it is appropriate for the new risk.

NOTE: In the above requirement, "significant" is deliberately not precisely defined. The definition used by an individual connected intersection may be specific to that connected intersection within constraints set by law, regulation, SCMS policy, etc. For further discussion, see the design section.

6.3.4.13.13 Security Validation

A connected intersection shall have a validation process that ensures that the security requirements of CTI 4501 are fulfilled, including on transition between different modes of operation.

6.3.4.13.14 Access Control on Internal CI Data Entities During Life Cycle

A connected intersection shall maintain appropriate access control during all of the following:

- Initial installation
- Maintenance or degraded operations
- System updates
- Software/firmware updates
- System outages

- Removal/decommissioning
- Performing security management on a CI data entity
- Entering or leaving a Maintenance Mode
- Power outages
- Recovery from disruption

NOTE: "Appropriate access control" can include being inaccessible until the CI data entity transitions out of the current state.

6.3.4.13.15 Maintenance Security Needs

A connected intersection shall manage its security mechanisms as part of the normal operations and maintenance (O&M) infrastructure supported by the IOO (possibly with additional training/tools and with the addition of a credential supplier as an additional supplier to the IOO).

6.3.4.13.16 Security Knowledge for Personnel

A connected intersection shall ensure that its personnel have sufficient security knowledge to manage reasonably foreseeable security incidents that require manual intervention.

6.3.4.14 Support Systems and Functions

The requirements for support systems and functions for a connected intersection follow.

NOTE: These requirements are system level and are in addition to the requirements on individual CI data entities given in 6.3.4.1. Communication of system monitoring or logging information from individual CI data entities to the system monitoring function is a CI data communication across a CI logical data interface (by the definition of those terms) and subject to the requirements given in 6.3.4.2. Data managed by the system monitoring system is CI data and components that have write or modify access to system monitoring data are CI data entities and the requirements of 6.3.4.1. apply to those components.

6.3.4.14.1 CI Performance Monitoring System

The connected intersection shall support a system monitoring function. This system monitoring function (CPMS) records the state of the system, including (a) hardware and software configuration of all CI data entities, (b) relevant version information, and (c) security-relevant events as specified in 6.3.4.14.2.

NOTE: Monitoring information is also CI data per the definition of CI data, and so access to the system’s diagnostic information is subject to the access control and other data-related security requirements of 6.3.4.1.

6.3.4.14.2 Events to be Monitored by the CPMS

The events covered by the CPMS shall include the following:

- Loss of network connection to any CI data entity
- Loss of power to any CI data entity
- Loss of input CI data to any CI data entity
- Loss of signing certificate validity on any appropriate CI data entity

- Failures of integrity of operation (see 6.3.4.1.8) on any CI data entity
- Integrity or authentication failures on CI data communications on any cryptographically protected CI data interface
- Failed user authentications, including excessive numbers of failed authentication attempts, to any CI data entity
- Access to - including modification or removal of - system and device logs (including who/what performed the access)
- Attempts of operators to invoke functions and services for which they are not authorized
- Modification of user/operator access rights and authenticators
- Excessive resource consumption events which may indicate a type of Denial-of-Service attack
- Modification of the diagnostic system’s configuration
- Interactions that are indicative of known cyberattacks

See 6.3.4.7, 6.3.4.8, and 6.3.4.9 on detecting incorrect SPaT, MAP, and RTCMcorrections messages.

NOTE: Each event is optional but strongly recommended.

6.3.4.14.3 CPMS: Other System Monitoring

The CPMS shall provide monitoring of system properties and events beyond the requirement of 6.3.4.14.2, as considered appropriate by the CI operator.

NOTE: This is optional because the CI operator may not consider additional events to be necessary to monitor.

6.3.4.14.4 CPMS: Robustness Against Invalid Input

The CPMS shall be robust against spoofing and other cyberattacks that would lead to it producing incorrect information.

"Incorrect information" in this context includes both detecting an error when there is no error and not detecting an error when there is an error.

This requirement is fulfilled by compliance with the communications security requirements of 6.3.4.2, if implemented (as required) on all inbound CI data logical interfaces to the system monitoring system, and the system robustness requirements of 6.3.4.13.

Per 6.3.4.1.42 and 6.3.4.1.43, data created or modified by the self-monitoring system is required to be stored in a robust and integrity-protected way.

6.3.4.14.5 CPMS: Error Management

A connected intersection shall implement mechanisms such that if the CPMS indicates an error that affects CI data, the connected intersection performs at least one of: (a) attempt to recover automatically; (b) directly notify an operator; (c) locally log the failure; (d) stop sending V2X messages or other CI data (which may apply to the CI data directly affected by the error or to any CI data downstream from it); or (e) inform receivers of that CI data that the data is not available or is suspect. Additional mitigations may also be implemented.

Monitoring information that is "reported out" per (b) above counts as CI data per the definition of CI data, and so the data communications for that information is subject to the data communications security requirements of 6.3.4.2.

6.3.4.15 Updates and Update Planning

The requirements for updates and update planning for a connected intersection follow.

NOTE: Requirements to track software version information for CI data entities are given in 6.3.4.1.8 and 6.3.4.14.1. Requirements for software update on CI data entities are given in 6.3.4.1. A device inside the connected intersection that can initiate a software update is a CI data entity per the definition of that term and so is subject to the access control requirements of 6.3.4.1. Some software update requirements that are implicit in the above requirements are stated explicitly in this section for clarity.

6.3.4.15.1 Prevent Unauthorized CI Software and Configuration Changes

The connected intersection shall include mechanisms to prevent unauthorized software updates and configuration changes.

6.3.4.15.2 Authenticate and Verify Integrity of All Software/Firmware Updates

A connected intersection shall authenticate, authorize, and verify the integrity of all software and firmware updates, including rollbacks to previously installed versions.

NOTE: This is optional because 6.3.4.1.47 requires each CI data entity to carry out these operations, and the connected intersection may consider it unnecessary to carry out additional validation before install.

6.3.4.15.3 CI Data Entity Update: Validation

A connected intersection shall implement mechanisms that validate the software/firmware update on a CI data entity before other CI data entities make use of CI data from the updated CI data entity.

6.3.4.15.4 CI Data Entity Update: Correct Status

A connected intersection shall implement mechanisms that ensure that it correctly reports software/firmware/configuration version status.

6.3.4.15.5 Tracking Evolution of CI-Related Standards

A connected intersection shall implement processes to track transition dates for CI-related standards impacting communications security and ensure that the connected intersection is updated in a timely manner to address each scheduled transition.

6.3.4.15.6 Tracking of Installed Version Information to CI-Related Standards

A connected intersection shall implement mechanisms that map the conformance of installed CI device and software/firmware versions to relevant CI-related standards impacting secure communications interoperability.

6.3.4.15.7 Update Cadence of CI Systems to CI-Related Standards

A connected intersection shall support CI-related communications security interoperability through the appropriate update of software to CI devices and applications to those standards according to their published transition dates.

6.3.4.16 System Operational Modes, Accesses, and Status

The requirements for system operational modes, accesses, and status for a connected intersection follow. See CTI 4501, 6.3.5.3 for definitions.

6.3.4.16.1 Correct Operational Mode Protection

The connected intersection shall be protected against operating in, transitioning to, or transitioning from Normal Mode when it should not.

6.3.4.16.2 Correct Mode and Status Reporting

A connected intersection shall implement mechanisms to prevent it from incorrectly reporting the operational mode or operational status of the system or its components.

6.3.4.16.3 Protection Against Improper Operation in Maintenance Mode

The connected intersection shall be protected against operating in, or transitioning to, Maintenance Mode or other non-normal modes when it should not.

6.3.4.16.4 Protecting Determinations that Normal Mode Transition Criteria are Met

The connected intersection shall include mechanisms to prevent an incorrect determination that conditions to transition to or from Normal Mode have been met.

6.3.4.16.5 Correct Representation of Operating Mode

The connected intersection shall include mechanisms to prevent an incorrect statement of the current operational mode.

6.3.4.17 V2X Message Transmission

The requirements for V2X message transmission for a connected intersection follow.

6.3.4.17.1 Prevent Change in Data Coverage

A connected intersection shall include mechanisms to prevent the data coverage from being changed such that messages can no longer be received in each lane approaching the intersection within the range of the ingress lane as identified in CTI 4501, 6.3.3.1.4.2, Advanced Notification - Time.

6.3.4.17.2 Detect Change in Data Coverage

A connected intersection shall include mechanisms to detect if the data coverage has been changed such that messages can no longer be received in each lane approaching the intersection within the range of the ingress lane as identified in CTI 4501, 6.3.3.1.4.2, Advanced Notification - Time.

6.3.4.17.3 Prevent Change in Radio Power

A connected intersection shall include mechanisms to prevent the radio transmit power from being lowered below a power level consistent with CTI 4501, 6.3.3.1.4.2.

6.3.4.17.4 Detect Change in Radio Power

A connected intersection shall include mechanisms to detect if the radio transmit power has been lowered below a power level consistent with CTI 4501, 6.3.3.1.4.2.

6.3.4.18 CI Security Verification Requirements

A connected intersection shall maintain documentation specifying how it conforms to these security requirements. This requirement also applies when material changes are made to implementations or operations that are relevant to these security requirements.

6.3.5 Operations and Maintenance Requirements

Not Applicable.

7. SYSTEM DESIGN

Section 7 defines the system design details based on the requirements identified in the Functional Requirements section (see Section 6). Section 7 includes the following:

a. A tutorial

b. A Requirements Traceability Matrix (RTM). The RTM links the requirements presented in Section 0 with the design details that describe how to fulfill each requirement. Using this table, each requirement can then be traced in a conformant way.

c. Design Details. Contains the details, guidance, and examples on how to fulfill a requirement.

Section 7 is intended for the following readers:

a. System integrators

b. Device manufacturers/vendors

c. Central system developers

d. Conformance testers

e. Other interested parties

For these readers, Section 7 is useful to understand how particular functions and information may be implemented to conform to CTI 4501.

7.1 Tutorial

The Requirements Traceability Matrix (RTM) in 7.2 identifies the design details that fulfill each of the requirements defined in Section 0. The design details that fulfill the requirements can be categorized as follows:

- Design details that do not require additional explanation. Some requirements do not require additional details on how to fulfill the requirement - those requirements are identified by "No Further Design Details" in the RTM.
- Design details that can be found in another reference.
- Design details that require additional guidance or explanation. These design details are found in Section 7.3.

7.2 Requirements Traceability Matrix (RTM)

The RTM links the requirements in Section 0 with the corresponding design details on the same line. Using this table, each requirement in Section 0 can thus be traced in a conformant way. Each requirement either points to other sections of the document where the formal design details on how to fulfill the requirement is described, provides no additional design details because the requirement is self-explanatory, or points to a normative reference that fulfills the requirement. In the latter case, the design details necessary to fulfill the requirement are contained within the normative reference.

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

7.2.1 Notation [Informative]

7.2.1.1 Functional Requirement Columns

The functional requirements are defined within Section 0, and the RTM is based upon the requirements within that section. The section number and the functional requirement name are indicated within these columns.

7.2.1.2 Design Details

The "Design Details" column either provides a hyperlinked reference to a section number where the design details are defined within 7.3, provides an external, normative reference that provides the details on how to fulfill the requirement, or indicates "No Further Design Details" because no additional design information is necessary (i.e., the requirement is self-explanatory).

7.2.1.3 Additional Specifications

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

7.2.2 Instructions for Completing the RTM [Informative]

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

Table 1 - Requirements Traceability Matrix (RTM)

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
6.3	Requirements		
6.3.1	Architectural Requirements		
		Refer to CTI 4501 Table 5, Requirements Traceability Matrix	
6.3.2	TSC Infrastructure to RSU Requirements	Not Applicable	
6.3.3	Message Requirements	Not Applicable	
6.3.4	Security Requirements		
6.3.4.1	Data Trustworthiness: Sources and Processing		
6.3.4.1.1	Internal Data Sources and Processing	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.2	Manual Data	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.3	Internal Manual Data Sources	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.4	Permitted Data from Manual Data Sources	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.5	External CI Data Entities	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.6	Authorized CI Data Entities	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.7	Authenticated CI Data Entities	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.8	Integrity of Operations for Internal CI Data Entities	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General See 7.3.4.1.2, Device-Level Protection of Integrity of Operations See 7.3.4.1.3.2, RSU Protection See 7.3.4.1.3.6, Factory Default See 0, 7.3.4.2.6.4.3Protection against TSC Infrastructure Reconfiguration from the RSU	
6.3.4.1.9	Integrity of Operational Mode for Internal CI Data Entities	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General See 7.3.4.1.3.9, Determine Mode of Operations See 7.3.4.1.3.10, Determine Operational Status See 7.3.4.1.3.11, Determine Operational Performance See 7.3.4.1.3.12, Determine Operating Environment	
6.3.4.1.10	Integrity of Operational Mode Indications for Internal CI Data Entities	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.11	Physical Access to Internal CI Data Entities	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General See 7.3.4.1.3.7, Protection against Tampering	
6.3.4.1.12	Physical Access to Internal CI Data Entities During Outages or Degraded Operations	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
6.3.4.1.13	Logical Access to Internal CI Data Entities	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General See 0, 7.3.4.1.3.3.2Password Change Prompt	
6.3.4.1.14	Logical Access to Internal CI Data Entities During Outages or Degraded Operations	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General See 7.3.4.1.3.4, Remote Restart	
6.3.4.1.15	Mitigate Malicious Access to Internal CI Data Entities	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.16	Access Control on Internal CI Data Entities During Life Cycle	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.17	Integrity of Operations for External CI Data Entities	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.18	Mitigate Malicious Access to External Data Sources and Processing	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.19	Access Privileges for Data Sources and Processing	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General See 0, 7.3.4.1.3.3.1Secure RSU Administration User Interface See 7.3.4.1.3.13, Access Control Policy	
6.3.4.1.20	Access Privileges for Manually Entered Data	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.21	Record of Accesses to CI Data Entities	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.24	Events to be Monitored by Self-Monitoring	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General See 7.3.4.1.3.5, Log Restarts See 7.3.4.1.3.8, Operational, Security, and other Events Logging - RSU	
6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.26	Self-Monitoring for Internal CI Data Entities: Robustness	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.27	Self-Monitoring for Internal CI Data Entities: Error Management	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.28	Recovery from Failure for Internal CI Data Entities	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.29	Assurance of Recovery from Failure for Internal CI Data Entities	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.30	Source Assurance for Recovery from Failure for Internal CI Data Entities	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
6.3.4.1.31	Automated Recovery from Failure for Internal CI Data Entities is Not to Be an Attack Vector	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.32	Self-Monitoring for Internal CI Data Entities: Logging	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.33	Log Generation for External CI Data Entities	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.34	Log Events for CI Data Entities	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.35	Changes in Logged Information	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.36	Access to Logs for CI Data Entities	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.37	Timely Access to Logs for CI Data Entities	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.38	List of Communications Nodes on which Data Could Be Modified	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.39	Communications Nodes on which Data is Manipulable Count as Data Transformation Components	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.40	Availability of CI Data	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.41	Mitigate Failures of Availability for CI Data	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.44	List of Privacy-Sensitive Information per CI Data Entity	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.45	Protecting Privacy-Sensitive Information per CI Data Entity	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General See 7.3.4.1.3.14, RSU Software and Firmware Updates See 7.3.4.1.3.15, Trustworthiness of Software and Firmware Updates See 7.3.4.1.4, TSC Protection: Infrastructure Software and Firmware Updates	
6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General See 7.3.4.1.3.14, RSU Software and Firmware Updates See 7.3.4.1.3.15, Trustworthiness of Software and Firmware Updates See 7.3.4.1.4, TSC Protection: Infrastructure Software and Firmware Updates	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General See 7.3.4.1.3.14, RSU Software and Firmware Updates See 7.3.4.1.3.15, Trustworthiness of Software and Firmware Updates See 7.3.4.1.4, TSC Protection: Infrastructure Software and Firmware Updates	
6.3.4.1.49	CI Data Entity Update: Validation	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General See 7.3.4.1.3.14, RSU Software and Firmware Updates See 7.3.4.1.3.15, Trustworthiness of Software and Firmware Updates See 7.3.4.1.4, TSC Protection: Infrastructure Software and Firmware Updates	
6.3.4.1.50	CI Data Entity Update: Correct Status	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General See 7.3.4.1.3.14, RSU Software and Firmware Updates See 7.3.4.1.3.15, Trustworthiness of Software and Firmware Updates See 7.3.4.1.4, TSC Protection: Infrastructure Software and Firmware Updates	
6.3.4.1.51	Protect V2X Radio Parameters	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.1.52	Threat Analysis	See 7.3.4.1.1, Connected Intersection Data Trustworthiness Design Details: General	
6.3.4.2	Data Communications Security		
6.3.4.2.1	List of Logical Interfaces	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization	
6.3.4.2.2	Secure Communications for CI Data Logical Interfaces	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
6.3.4.2.3	Secure Communications: Integrity	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization	
6.3.4.2.4	Secure Communications: Integrity of External CI Data Outbound Logical Interfaces	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization	
6.3.4.2.5	Secure Communications: Replay Protection	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization	
6.3.4.2.6	Secure Communications: Plausibility for Received Data	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
6.3.4.2.7	Secure Communications: CI-Internal Logical Component Authentication	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization	
6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization	
6.3.4.2.9	Secure Communications: Authentication of External CI Data Logical Interfaces	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization	
6.3.4.2.10	Secure Communications: Authentication of External CI Data Outbound Logical Interfaces	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
6.3.4.2.11	Secure Communications: Check Authentication for Received Data	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization See 7.3.4.2.11.1, Monitor Certificate Status See 7.3.4.2.12.2, Download SCMS Files	
6.3.4.2.12	Secure Communications: Manage Received Data for Which Checks Have Failed	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization See 7.3.4.2.11.2, Drop Connections	
6.3.4.2.13	Secure Communications: External Data Entities for Which Checks Have Failed	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
6.3.4.2.14	Secure Communications: Other Users of External Data Entities for Which Checks Have Failed	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization See 7.3.4.1.3.1, Management of RSU X.509 Credentials	
6.3.4.2.15	Entitlement to Authentication Credentials	See 7.3.4.1.3.1, Management of RSU X.509 Credentials See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.4, 1609.2 Certificate Issuance See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization	
6.3.4.2.16	Secure Issuance of Authentication Credentials	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.2, Interface between RSU and SCMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization See 7.3.4.2.10.2, Credential Updates See 7.3.4.2.12.1, Connectivity Design	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
6.3.4.2.17	Secure Re-Issuance of Authentication Credentials	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization	
6.3.4.2.18	Blocking Re-Issuance of Authentication Credentials	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.5, 1609.2 Certificate Non-Issuance See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization	
6.3.4.2.19	List of Privacy-Sensitive Information Flows	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
6.3.4.2.20	Protecting Privacy-Sensitive Information Flows	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization	
6.3.4.2.21	Protecting Sent Privacy-Sensitive Information when Received	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization	
6.3.4.2.22	Security Size Overhead	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization	
6.3.4.2.23	Security Processing Overhead	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
6.3.4.2.24	Protection of Cryptographic Keying Material: General	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization See 7.3.4.7.2, SPaT Message Signing	
6.3.4.2.25	Protection of Cryptographic Keying Material: Hardware	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization See 7.3.4.7.2, SPaT Message Signing	
6.3.4.2.26	Protection of Cryptographic Keying Material: Access to and Use of Keys	See 7.3.4.2.2, Secure Network See 7.3.4.2.3, Assurance of Connection to Correct Network See 7.3.4.2.6.1, Interface between RSU and TMS See 7.3.4.2.6.3, Interface between an RSU and the OBU/MU See 0, 7.3.4.2.6.4.1Use of Secure Transport Protocol See 0, 7.3.4.2.6.4.2Use of (D)TLS Protocol See 7.3.4.2.7, Interface between the TMS and the TSC Infrastructure See 7.3.4.2.8, Interface between the MAP Server and the TMS See 7.3.4.2.9, Interface between MAP Server and the SCMS See 7.3.4.2.10.1, Start-up Initialization See 7.3.4.7.2, SPaT Message Signing	
6.3.4.3	Trustworthiness of TSC-Originating Information		
6.3.4.3.1	TSC Infrastructure Protection: Invalid Signal Timing Information	See 7.3.4.3.1, Trustworthiness of TSC-Originating Information: General	
6.3.4.3.2	TSC Infrastructure Protection: Invalid Format for Signal Timing Information	See 7.3.4.3.1, Trustworthiness of TSC-Originating Information: General	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
6.3.4.3.3	TSC Infrastructure Protection: Incorrect Format for Signal Timing Information	See 7.3.4.3.1, Trustworthiness of TSC-Originating Information: General	
6.3.4.3.4	TSC Infrastructure Protection: Invalid Contents for Signal Timing Data	See 7.3.4.3.1, Trustworthiness of TSC-Originating Information: General	
6.3.4.3.5	Information About Availability of SPaT Information	See 7.3.4.3.1, Trustworthiness of TSC-Originating Information: General	
6.3.4.4	Approaching Vehicle Information Trustworthiness: RSU		
6.3.4.4.1	Validate Security of Approaching Vehicle V2X Messages	See 7.3.4.4.1, Approaching Vehicle Information Trustworthiness: RSU: General See 7.3.4.4.2, 1609.2 Validation of BSMs	
6.3.4.4.2	Validate Approaching Vehicle V2X Messages: Replay	See 7.3.4.4.1, Approaching Vehicle Information Trustworthiness: RSU: General See 7.3.4.4.3, Replay	
6.3.4.4.3	Validate Approaching Vehicle V2X Messages: Misbehavior Detection	See 7.3.4.4.1, Approaching Vehicle Information Trustworthiness: RSU: General See 7.3.4.4.4, Misbehavior Detection	
6.3.4.4.4	Validate Approaching Vehicle V2X Messages: Misbehavior Reporting	See 7.3.4.4.1, Approaching Vehicle Information Trustworthiness: RSU: General See 7.3.4.4.5, Misbehavior Reporting (OPTIONAL) See 7.3.4.4.6, Misbehavior Reporting: Certificate (MANDATORY if 7.3.4.4.5 is implemented)	
6.3.4.4.5	Validate Approaching Vehicle V2X Messages: Distinguish Between Senders	See 7.3.4.4.1, Approaching Vehicle Information Trustworthiness: RSU: General	
6.3.4.4.6	Security for Use of RSU BSM Filtering for RDZ	See 7.3.4.4.1, Approaching Vehicle Information Trustworthiness: RSU: General	
6.3.4.4.7	Security for Configuration of RSU BSM Filtering for RDZ	See 7.3.4.4.1, Approaching Vehicle Information Trustworthiness: RSU: General	
6.3.4.5	Approaching Vehicle Information Trustworthiness and AGP: TSC		
6.3.4.5.1	Protection from Unnecessary AGP	See 7.3.4.5.1, Approaching Vehicle Information Trustworthiness: TSC: General	
6.3.4.6	Time Source Trustworthiness		
6.3.4.6.1	Availability of Time Sources	See 7.3.4.6.1, Time Source Trustworthiness: Design Details: General	
6.3.4.6.2	Detect Time Source Delay	See 7.3.4.6.1, Time Source Trustworthiness: Design Details: General	
6.3.4.6.3	Manage Time Source Delay	See 7.3.4.6.1, Time Source Trustworthiness: Design Details: General	
6.3.4.6.4	Time Source Delay for External Time Sources	See 7.3.4.6.1, Time Source Trustworthiness: Design Details: General	
6.3.4.6.5	Time Source Delay for External Time Sources: Other Users	See 7.3.4.6.1, Time Source Trustworthiness: Design Details: General	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
6.3.4.7	SPaT Message Trustworthiness and Reliability		
6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents	See 7.3.4.7.1, SPaT Message Trustworthiness and Reliability: Design Details: General	
6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior	See 7.3.4.7.1, SPaT Message Trustworthiness and Reliability: Design Details: General	
6.3.4.7.3	Detect Inconsistency of SPaT and Signal Timing Data	See 7.3.4.7.1, SPaT Message Trustworthiness and Reliability: Design Details: General	
6.3.4.7.4	Manage Inconsistency of SPaT and Signal Timing Data	See 7.3.4.7.1, SPaT Message Trustworthiness and Reliability: Design Details: General	
6.3.4.8	MAP Message Contents Trustworthiness		
6.3.4.8.1	List of CI Data Entities that Affect MAP Contents	See 7.3.4.8.1, MAP Message Trustworthiness and Reliability: Design Details: General	
6.3.4.8.2	Prevent Invalid MAP Contents or Behavior	See 7.3.4.8.1, MAP Message Trustworthiness and Reliability: Design Details: General	
6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source	See 7.3.4.8.1, MAP Message Trustworthiness and Reliability: Design Details: General	
6.3.4.8.4	Prevent Inconsistency of MAP and Road Geometry or Use: False Positives	See 7.3.4.8.1, MAP Message Trustworthiness and Reliability: Design Details: General	
6.3.4.8.5	Prevent Inconsistency of MAP and Road Geometry or Use: False Negatives	See 7.3.4.8.1, MAP Message Trustworthiness and Reliability: Design Details: General	
6.3.4.8.6	Detect Inconsistency of MAP and Road Geometry or Use	See 7.3.4.8.1, MAP Message Trustworthiness and Reliability: Design Details: General	
6.3.4.8.7	Manage Inconsistency of MAP and Road Geometry or Use	See 7.3.4.8.1, MAP Message Trustworthiness and Reliability: Design Details: General	
6.3.4.9	RTCM Message Contents Trustworthiness		
6.3.4.9.1	List of CI Data Entities that Affect RTCM Contents	See 7.3.4.9.1, RTCM Message Trustworthiness and Reliability: Design Details: General See 7.3.4.9.2, RTCM Corrections Data Trustworthiness	
6.3.4.9.2	Prevent Invalid RTCM Contents or Behavior	See 7.3.4.9.1, RTCM Message Trustworthiness and Reliability: Design Details: General See 7.3.4.9.2, RTCM Corrections Data Trustworthiness	
6.3.4.9.3	External RTCM Message Generation or Partial Generation: Data Source	See 7.3.4.9.1, RTCM Message Trustworthiness and Reliability: Design Details: General See 7.3.4.9.2, RTCM Corrections Data Trustworthiness	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
6.3.4.10	Consistency Between MAP and SPaT Messages		
6.3.4.10.1	SPaT and MAP Version Consistency	See 7.3.4.10, Consistency between MAPs and SPaTs: Design Details	
6.3.4.10.2	SPaT and MAP Intersection Identifier Consistency	See 7.3.4.10, Consistency between MAPs and SPaTs: Design Details	
6.3.4.11	Unavailability Indications		
6.3.4.11.1	Correctness of SPaT Availability Indications	See 7.3.4.11.1, Unavailability Indications: Design Details: General	
6.3.4.11.2	Correctness of SPaT Unavailability Indications	See 7.3.4.11.1, Unavailability Indications: Design Details: General	
6.3.4.11.3	Correctness of MAP Availability Indications	See 7.3.4.11.1, Unavailability Indications: Design Details: General	
6.3.4.11.4	Correctness of MAP Unavailability Indications	See 7.3.4.11.1, Unavailability Indications: Design Details: General	
6.3.4.12	Intersection Identifier Trustworthiness		
6.3.4.12.1	Robustness of Intersection Identifier Assignment	See 7.3.4.12.1, Intersection Identifier Trustworthiness: Design Details: General	
6.3.4.12.2	Detect Incorrect Intersection Identifiers	See 7.3.4.12.1, Intersection Identifier Trustworthiness: Design Details: General	
6.3.4.12.3	Manage Incorrect Intersection Identifiers	See 7.3.4.12.1, Intersection Identifier Trustworthiness: Design Details: General	
6.3.4.12.4	Detect Duplicate Use of Intersection Identifiers by External Parties	See 7.3.4.12.1, Intersection Identifier Trustworthiness: Design Details: General	
6.3.4.12.5	Manage Duplicate Use of Intersection Identifiers by External Parties	See 7.3.4.12.1, Intersection Identifier Trustworthiness: Design Details: General	
6.3.4.13	System Management and Recovery		
6.3.4.13.1	System Recovery - Software and Configuration Backups	See 7.3.4.13.1, System Management and Recovery: Design Details: General	
6.3.4.13.2	List of Operator-Notifiable Events	See 7.3.4.13.1, System Management and Recovery: Design Details: General	
6.3.4.13.3	List of Systemic Failure Events	See 7.3.4.13.1, System Management and Recovery: Design Details: General	
6.3.4.13.4	Cyberattack Must be Addressed	See 7.3.4.13.1, System Management and Recovery: Design Details: General See 7.3.4.13.3.1, Cyberattack Recovery Plan See 7.3.4.13.3.2, Cyberattack Robustness	
6.3.4.13.5	Recovery Plan from Systemic Failure	See 7.3.4.13.1, System Management and Recovery: Design Details: General	
6.3.4.13.6	Recovery from Systemic Failure Only When Necessary	See 7.3.4.13.1, System Management and Recovery: Design Details: General	
6.3.4.13.7	Preserve Access Control During Systemic Failure	See 7.3.4.13.1, System Management and Recovery: Design Details: General	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
6.3.4.13.8	Robustness of Recovery from Systemic Failure	See 7.3.4.13.1, System Management and Recovery: Design Details: General	
6.3.4.13.9	Assurance of Recovery from Systemic Failure	See 7.3.4.13.1, System Management and Recovery: Design Details: General	
6.3.4.13.10	Source Assurance for Recovery from Failure for Internal Data Sources or Processors	See 7.3.4.13.1, System Management and Recovery: Design Details: General	
6.3.4.13.11	Automated Recovery from Failure for the CI is not to be an Attack Vector	See 7.3.4.13.1, System Management and Recovery: Design Details: General	
6.3.4.13.12	Vulnerability Management for Potential	See 7.3.4.13.1, System Management and Recovery: Design Details: General	
6.3.4.13.13	Security Validation	See 7.3.4.13.1, System Management and Recovery: Design Details: General	
6.3.4.13.14	Access Control on Internal CI Data Entities During Life Cycle	See 7.3.4.13.1, System Management and Recovery: Design Details: General	
6.3.4.13.15	Maintenance Security Needs	See 7.3.4.13.1, System Management and Recovery: Design Details: General	
6.3.4.13.16	Security Knowledge for Personnel	See 7.3.4.13.1, System Management and Recovery: Design Details: General See 7.3.4.13.2, CI Operation Security Practices	
6.3.4.14	Support Systems and Functions		
6.3.4.14.1	CI Performance Monitoring System	See 7.3.4.13.4.1, Network Protection See 7.3.4.14.1, Support Systems and Functions: Design Details: General See 7.3.4.15.1, Updates and Update Planning: Design Details: General See 7.3.4.16.1, System Operational Modes, Accesses, and Status: Design Details: General See 7.3.4.17.1, V2X Message Transmission: Design Details: General	
6.3.4.14.2	Events to be Monitored by	See 7.3.4.14.1, Support Systems and Functions: Design Details: General See 7.3.4.15.1, Updates and Update Planning: Design Details: General See 7.3.4.16.1, System Operational Modes, Accesses, and Status: Design Details: General See 7.3.4.17.1, V2X Message Transmission: Design Details: General	
6.3.4.14.3	CPMS: Other System Monitoring	See 7.3.4.14.1, Support Systems and Functions: Design Details: General See 7.3.4.15.1, Updates and Update Planning: Design Details: General See 7.3.4.16.1, System Operational Modes, Accesses, and Status: Design Details: General See 7.3.4.17.1, V2X Message Transmission: Design Details: General	
6.3.4.14.4	CPMS: Robustness Against Invalid Input	See 7.3.4.14.1, Support Systems and Functions: Design Details: General See 7.3.4.15.1, Updates and Update Planning: Design Details: General See 7.3.4.16.1, System Operational Modes, Accesses, and Status: Design Details: General See 7.3.4.17.1, V2X Message Transmission: Design Details: General	

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
6.3.4.14.5	CPMS: Error Management	See 7.3.4.14.1, Support Systems and Functions: Design Details: General See 7.3.4.15.1, Updates and Update Planning: Design Details: General See 7.3.4.16.1, System Operational Modes, Accesses, and Status: Design Details: General See 7.3.4.17.1, V2X Message Transmission: Design Details: General	
6.3.4.15	Updates and Update Planning		
6.3.4.15.1	Prevent Unauthorized CI Software and Configuration Changes		
6.3.4.15.2	Authenticate and Verify Integrity of All Software/Firmware Updates		
6.3.4.15.3	CI Data Entity Update: Validation		
6.3.4.15.4	CI Data Entity Update: Correct Status		
6.3.4.15.5	Tracking Evolution of CI-Related Standards		
6.3.4.15.6	Tracking of Installed Version Information to CI-Related Standards		
6.3.4.15.7	Update Cadence of CI Systems to CI-Related Standards		
6.3.4.16	System Operational Modes, Accesses, and Status		
6.3.4.16.1	Correct Operational Mode Protection		
6.3.4.16.2	Correct Mode and Status Reporting		
6.3.4.16.3	Protection Against Improper Operation in Maintenance Mode		
6.3.4.16.4	Protecting Determinations that Normal Mode Transition Criteria are Met		
6.3.4.16.5	Correct Representation of Operating Mode		
6.3.4.17	V2X Message Transmission		
6.3.4.17.1	Prevent Change in Data Coverage		
6.3.4.17.2	Detect Change in Data Coverage		
6.3.4.17.3	Prevent Change in Radio Power		
6.3.4.17.4	Detect Change in Radio Power		
6.3.4.18	CI Security Verification Requirements	See 7.3.4.18.1, Security Compliance Assessment	
6.3.5	Operations and Maintenance Requirements		
6.3.5.1	Interoperability Requirements		

Requirements Traceability Matrix (RTM)			
FR ID	**Functional Requirement**	**Design Detail**	**Additional Specification**
6.3.5.1.1	Mean-Time-Between-Failures (MTBF)		
6.3.5.1.2	Operational Uptime		
6.3.5.1.3	Continuous Operation		
6.3.5.1.4	Continue to Transmit MAP Messages		
6.3.5.2	Life Cycle Requirements		
6.3.5.2.1	Documented Plan for Lifecyle Operations & Maintenance		
6.3.5.3	Maintenance Requirements		
6.3.5.3.1	Support Normal Mode		
6.3.5.3.2	Maintenance Mode		
6.3.5.3.3	Report Operational Mode Status		
6.3.5.3.4	Support Maintenance Mode Fallback		
6.3.5.3.5	Perform Validation		
6.3.5.3.6	Command Maintenance Mode		
6.3.5.3.7	Automatic Return to Normal Mode		
6.3.5.4	System Diagnostic Interface Requirements		
6.3.5.4.1	System Malfunction Alert		
6.3.5.4.2	Detect System Exceptions		
6.3.5.4.3	System Exception Reporting		
6.3.5.4.4	System Component Diagnostics		
6.3.5.5	CPMS Requirements		
6.3.5.5.1	Support Monitoring System		
6.3.5.5.2	Support Maintenance Mode in Monitoring		
6.3.5.6	System Upgradeability Requirements		
6.3.5.6.1	Support Software Updates		
6.3.5.7	System Recovery Requirements		
6.3.5.7.1	Support Operational Mode Following Recovery		
6.3.5.7.2	Device Power Interruption Recovery		
6.3.5.7.3	Restore Communications Automatically		
6.3.5.7.4	Process Recovery		

7.3 Design Details

The design details to fulfill the requirements defined in Section 0 follow.

7.3.1 Architectural Design Details

Not applicable.

7.3.2 TSC Infrastructure to RSU Design Details

Not applicable.

7.3.3 Message Design Details

Not applicable.

7.3.4 Security Design Details

The design details to fulfill the security requirements for a connected intersection follow. These requirements are defined in 6.3.4.

7.3.4.1 Connected Intersection Data Trustworthiness Design Details

The design details to fulfill the requirements for sources and processing data trustworthiness for a connected intersection follow.

7.3.4.1.1 Connected Intersection Data Trustworthiness Design Details: General

A connected intersection shall fulfill the requirements of 6.3.4.1 by the means specified in this section or by vendor-specific means in the case where this section does not give specific design details. The CI operator shall create documentation that documents how those requirements are met.

This documentation shall include at least the following:

A list of all internal CI data entities per 6.3.4.1.1 and all external CI data entities per 6.3.4.1.5, including components that are to be considered data entities per 6.3.4.1.38 and 6.3.4.1.39.

For each data entity:

- How it establishes authenticity and authorization per 6.3.4.1.6, 6.3.4.1.7
- How the system mitigates the effects of unauthorized access per 6.3.4.1.15, 6.3.4.1.18
- For each internal CI data entity:
    - Whether it supports manual data entry and, if so, how the relevant security requirements are fulfilled per 6.3.4.1.2, 6.3.4.1.3, 6.3.4.1.4
    - How integrity of operations is protected per 6.3.4.1.8, 6.3.4.1.9, 6.3.4.1.10, including an analysis of threats to integrity of operations and how they are mitigated
    - How physical access is secured per 6.3.4.1.11, 6.3.4.1.12, 6.3.4.1.16
    - How logical access is secured per 6.3.4.1.13, 6.3.4.1.14, 6.3.4.1.16
    - How access privileges are managed and what access privileges each user of the system currently has, per 6.3.4.1.19, 6.3.4.1.20

- How self-monitoring and logging are implemented and how the self-monitoring and logging systems are ensured to be robust, correct, and not a potential attack vector per 6.3.4.1.23, 6.3.4.1.24, 6.3.4.1.25, 6.3.4.1.26, 6.3.4.1.27, 6.3.4.1.32, 6.3.4.1.34, 6.3.4.1.35, 6.3.4.1.36, 6.3.4.1.37
- How it recovers from error states per 6.3.4.1.28, 6.3.4.1.29, 6.3.4.1.30, 6.3.4.1.31
- How the system mitigates the risk that input data is unavailable per 6.3.4.1.40, 6.3.4.1.41
- How the system mitigates the risk that stored data is corrupted per 6.3.4.1.42, 6.3.4.1.43
- Whether it manages privacy-sensitive information and, if so, how that information is protected per 6.3.4.1.44, 6.3.4.1.45
- How updates are secured per 6.3.4.1.46, 6.3.4.1.47, 6.3.4.1.48, 6.3.4.1.49, 6.3.4.1.50
- How radio parameters are protected from modification per 6.3.4.1.51
- How remaining non-negligible threats are mitigated per 6.3.4.1.52.
- If the CI data entity uses cryptographic authentication keys, how they are protected per 6.3.4.2.24, 6.3.4.2.25, 6.3.4.2.26

- For each external CI data entity:
  - A note that assurance has been received regarding integrity of operations per 6.3.4.1.17
  - A note that appropriate logging is implemented per 6.3.4.1.33

The CI operator shall self-assert that this security documentation exists and has been correctly completed.

The current document does not create a requirement that the security documentation is shared with any party outside the CI. However, there may be requirements that some security documentation is shared. These requirements could be created by the SCMS provider, by regulation, by public policy, or by any other relevant means. If sharing is required, it could take many forms, including sharing confidentially with an auditor or third-party analyst, sharing the documentation with the SCMS provider, or publishing some or all of the documentation online for inspection. The current document does not make any assumptions about the form of sharing, if any. It is the responsibility of the CI operator to understand what level of validation of the security documentation is required and what sharing is necessary to support validation or for other purposes.

These security documentation requirements are anticipated to change over time. While self-declaration is currently acceptable, the security compliance assessment documentation requirements themselves may change over time (for example, becoming more specific), and self-declaration may be replaced by a certification process involving an external party. As such, the IOO shall identify which version of CTI 4501 the security compliance assessment documentation conforms with. Doing so may mitigate deployment delays associated with compliance security assessment documentation that may not conform to later requirements. Annex B provides an example process of how an IOO may prepare its security compliance assessment documentation.

7.3.4.1.2 Device-Level Protection of Integrity of Operations

For each CI data entity, a connected intersection shall fulfil the requirement of 6.3.4.1.8 by any vendor-specific means. For example, a Certificate Authority (CA) data entity might employ malware and intrusion detection and protection; IP-level firewall (e.g., iptables) supporting at a minimum closing of all unused ports by default and opening the NTCIP 1218 port for outgoing connections only; or the CI data entity might not implement these controls itself but might be operating in an environment that provides equivalent controls.

7.3.4.1.3 RSU Security Standards

7.3.4.1.3.1 Management of RSU X.509 Credentials

The RSU shall comply with CTI 4001, 4.3.5.12, Secure Management of X.509 Credentials for TLS.

TRACEABILITY: 6.3.4.2.14, 6.3.4.2.15

7.3.4.1.3.2 RSU Protection

The RSU shall comply with CTI 4001, 4.3.5.8, RSU Operating System Security Design Details. This includes support for disabling unused applications and services (refer to CTI 4001, 4.3.5.8.1, RSU OS Applications and Services Design Details therein). This includes temporarily blocking/closing unused IP ports (refer to CTI 4001, 4.3.5.8.2, RSU OS Ports and Protocols Design Details therein).

If the RSU provides additional protections, for example blocking individual source IP addresses, this shall be documented in the security documentation.

NOTE: If the RSU blocks individual source IP addresses, care should be taken that an attacker cannot use this mechanism to trick the RSU into blocking communications from the TSC infrastructure or from the TMS.

7.3.4.1.3.3 Secure Administration of RSU

The design details to fulfill the requirements to provide secure administration of an RSU follow. These requirements are defined in 6.3.4.1.

7.3.4.1.3.3.1 Secure RSU Administration User Interface

The RSU shall comply with CTI 4001, 4.3.5.11, Secure Administration Design Details.

7.3.4.1.3.3.2 Password Change Prompt

If the RSU provides a web-based administration user interface, the RSU shall comply with CTI 4001, 4.3.5.11.1.2, Secure Administration - Web-Based Access Design Details.

NOTE: The referenced section requires that the password be changed from the default password.

If the RSU provides an SSH-based administration command line interface, the RSU shall comply with CTI 4001, 4.3.5.11.1.3, Secure Administration - SSH Design Details.

NOTE: The referenced section requires that the password be changed from the default password.

7.3.4.1.3.4 Remote Restart

The RSU shall comply with CTI 4001, 3.3.2.1.2, RSU Restarts.

7.3.4.1.3.5 Log Restarts

The RSU shall comply with CTI 4001, 4.3.2.3, Log Restarts Design Details.

7.3.4.1.3.6 Factory Default

The RSU shall comply with CTI 4001, 4.3.2.2, Factory Default Design Details.

7.3.4.1.3.7 Protection against Tampering

The RSU shall comply with CTI 4001, 4.3.5.6.1, Tamper Evident Enclosure - Visual Design Details.

The RSU shall comply with CTI 4001, 4.3.5.6.2, Tamper Evident Port Design Details.

7.3.4.1.3.8 Operational, Security, and other Events Logging - RSU

The RSU shall comply with CTI 4001, 4.3.5.13, Logging for General and Security Purposes Design Details.

7.3.4.1.3.9 Determine Mode of Operations

The RSU shall comply with CTI 4001, 3.3.3.2.1, Determine Mode of Operations.

7.3.4.1.3.10 Determine Operational Status

The RSU shall comply with CTI 4001, 4.3.3.1, Monitor Current Status Design Details.

7.3.4.1.3.11 Determine Operational Performance

The RSU shall comply with CTI 4001, 3.3.3.2.3, Determine Operational Performance.

7.3.4.1.3.12 Determine Operating Environment

The RSU shall comply with CTI 4001, 3.3.3.2.4, Determine Operating Environment.

7.3.4.1.3.13 Access Control Policy

Tasks on the RSU requiring administrative privileges include the following:

- Install the public cert and private key
- Install a chain of trust
- Perform (re-) enrollment into an SCMS
- Write/modify access control policies
- Write/modify information flow control policies
- Write the list of auditable activities
- Delete audit log data
- Install software other than signed software whose signature chains to a verification key whose integrity is protected by hardware on the device
- Changes to SPAT parameters on the RSU, which affect the content of the broadcast SPAT messages

If the RSU supports these tasks via its NTCIP 1218 interface, then it shall be configured such that only an administrator (i.e., an administrative SNMP user) is allowed to perform these tasks in order to comply with this requirement.

If the RSU supports these tasks via its administration interface as specified in CTI 4001, 4.3.5.11, Secure Administration Design Details, then the RSU complies with this requirement.

The RSU shall support ongoing privileged access by requiring periodic re-authentication of administrator privileges, with a recommended interval of at least once every hour.

NOTE: This is to guard against privilege escalation attacks.

These tasks above shall only be carried out if all of the following conditions are met:

- The administrator used a password that fulfills the requirements for administrative accounts as in the CTI 4001, 4.3.5.8.3, RSU Password Design Details.
- The administrator is logged into the RSU directly or via a secure connection using TLS 1.3 or DTLS 1.3 with mutual authentication and client-side certificates.
- The secure session is fresh, i.e., it is torn down after a configurable period of user inactivity (e.g., time-out of 2 minutes). When a login session expires, a re-authentication is required.

7.3.4.1.3.14 RSU Software and Firmware Updates

The RSU shall comply with CTI 4001, 3.3.1.14, Software and Firmware Updates Requirements.

7.3.4.1.3.15 Trustworthiness of Software and Firmware Updates

The RSU shall implement a vendor-specific mechanism fulfilling all of the following requirements:

- The RSU shall only install software and firmware updates which are signed by the RSU manufacturer.
- Update packages shall be authenticated by the RSU before installation.
- Unauthorized rollbacks to previous updates shall be prevented.
- The RSU software update system shall protect software update authentication keys from compromise.

7.3.4.1.4 TSC Protection: Infrastructure Software and Firmware Updates

The TSC infrastructure shall implement a vendor-specific mechanism fulfilling all of the following requirements:

- The TSC infrastructure components shall only install software and firmware updates which are either: signed by the TSC component manufacturer; or signed by the IOO (or simply provided by IOO and installed by a user with admin privileges) and then described in documentation. Update packages shall be authenticated by the TSC component before installation.
- Unauthorized rollbacks to previous updates shall be prevented.
- The TSC infrastructure software update system shall protect software update authentication keys from compromise.

If the TSC infrastructure elements are from different manufacturers, then the updates may come from more than one source. It is important for the CI system to ensure that every component only accepts authenticated updates verifiably originated from its own manufacturer (and verified by the CI system to enact changes as intended).

7.3.4.2 Connected Intersection Data Communications Security Design Details

The design details to fulfill data communications security requirements for a connected intersection follow.

7.3.4.2.1 Connected Intersection Data Communications Security Design Details: General

A connected intersection shall fulfill the requirements of 6.3.4.2 by the means specified in this section or by vendor-specific means in the case where this section does not give specific design details. The CI operator shall create documentation that documents how those requirements are met.

This documentation shall include at least the following:

- A list of all logical interfaces per 6.3.4.2.1
- For each logical interface:
    - Whether or not it is a cryptographically protected logical interface per 6.3.4.2.2
- For each not cryptographically protected logical interface:
    - A statement of what other protection mechanism is used
    - A statement of whether the interface is one of the identified exception cases for which cryptographic protection is not necessary
    - How it implements the plausibility checks of 6.3.4.2.6 and what action is taken if those checks fail, per 6.3.4.2.12
- For each cryptographically protected logical interface:
    - A statement of what cryptographic protection is used and how it fulfills the performance requirements of 6.3.4.2.22 and 6.3.4.2.23
    - How it implements the security checks of 6.3.4.2.3, 6.3.4.2.4, 6.3.4.2.5, 6.3.4.2.6, 6.3.4.2.7 (if applicable), 6.3.4.2.8 (optionally and if applicable), 6.3.4.2.9 (if applicable), 6.3.4.2.10 (if applicable), 6.3.4.2.11
    - How the receiver reacts if incoming messages fail any of the checks per 6.3.4.2.12, 6.3.4.2.13 (if applicable), 6.3.4.2.14 (if applicable)
    - Whether the information sent across the interface is privacy-sensitive per 6.3.4.2.19
- For each cryptographically protected logical interface across which privacy-sensitive information is sent, in addition to the requirements above:
    - How privacy-sensitive information is protected from exposure in transit across the interface per 6.3.4.2.20
    - How privacy-sensitive information is protected from exposure once received per 6.3.4.2.21
- For each CI data entity that sends data across a cryptographically secure logical interface:
    - The policy to be followed in issuing credentials to the CI data entity per 6.3.4.2.15
    - The credential issuance and re-issuance process per 6.3.4.2.16, 6.3.4.2.17
    - The process to notify the credential issuer that credentials should be blocked per 6.3.4.2.18

The CI operator shall self-assert that this security documentation exists and has been correctly completed.

The current document does not create a requirement that the security documentation is shared with any party outside the CI. However, there may be requirements that some security documentation is shared. These requirements could be created by the SCMS provider, by regulation, by public policy, or by any other relevant means. If sharing is required, it could take many forms, including sharing confidentially with an auditor or third-party analyst, sharing the documentation with the SCMS provider, or publishing some or all of the documentation online for inspection. The current document does not make any assumptions about the form of sharing, if any. It is the responsibility of the CI operator to understand what level of validation of the security documentation is required and what sharing is necessary to support validation or for other purposes.

These security documentation requirements are anticipated to change over time. While self-declaration is currently acceptable, the security compliance assessment documentation requirements themselves may change over time (for example, becoming more specific), and self-declaration may be replaced by a certification process involving an external party. As such, the IOO shall identify which version of CTI 4501 the security compliance assessment documentation conforms with. Doing so may mitigate deployment delays associated with compliance security assessment documentation that may not conform to later requirements. Annex B provides an example process of how an IOO may prepare its security compliance assessment documentation.

NOTE: For specific interfaces (e.g., TSC-RSU or the logical interface used by TMC to configure the RSU), more specific design details are given below and implementation of those design details fulfills the appropriate requirements referenced by this section.

7.3.4.2.2 Secure Network

The center servers (TMS, Map Data Server, and any RTCM or External control system) shall employ transport-level security in all of their interfaces that might affect CI data.

A TMS shall implement SNMPv3 as required to support NTCIP 1218 objects.

A TMS shall implement SSH 2.0 as specified in RFC 4253.

These servers shall support TLS 1.3 as specified in CTI 4001, 4.3.5.2, Local and Back-Office Interface Security Design Details. If DTLS is more appropriate than TLS and is consistent with other standards in use with the system (for example, NTCIP standards), then DTLS may be used. This document permits the use of both DTLS 1.2 and DTLS 1.3.

These servers shall not implement unsecured communication using HTTP for any communications that might affect CI data.

7.3.4.2.3 Assurance of Connection to Correct Network

The RSU shall ensure it is connected to the correct TMS and the TSC infrastructure by implementing the design specified in 7.3.4.2.6.1, Interface between RSU and TMS, and 7.3.4.2.6.4, Interface between an RSU and the TSC Infrastructure, respectively.

This requirement does not apply to the TMS (and MAP server if applicable), since they have assurance to be connected to the correct network by being physically part of the IOO network.

7.3.4.2.4 1609.2 Certificate Issuance

While third-party assessment is expected in the future, currently the organization responsible for signing SPaT and MAP messages shall provide a self-declaration of having met the security requirements contained in this document to the SCMS provider they have selected. The SCMS provider shall then issue certificates.

It is expected that in the future, the requirement will be to obtain one or more certifications from third parties that will need to be submitted in addition to self-declarations for items not covered in those certifications.

7.3.4.2.5 1609.2 Certificate Non-Issuance

It is the responsibility of the IOO to ensure that their system initially complies with the security requirements and continues to do so in operation. The IOO asserts compliance to the SCMS provider by providing a self-declaration that the connected intersection fulfills these requirements. If the IOO discovers that parts of the system no longer comply with the security requirements, the IOO is required to notify the SCMS provider. Devices affected by this non-compliance are no longer eligible for IEEE Std 1609.2 certificates, and the SCMS provider is expected to no longer issue IEEE Std 1609.2 certificates to those devices until the non-compliance is addressed and the SCMS provider is notified that those parts of the system are now back in compliance.

NOTE: In the future, it is expected that self-declaration will not be acceptable on its own and that the IOO will be required to acquire certifications from one or more third parties and present those certifications to the SCMS in order to receive IEEE Std 1609.2 certificates. Deployers are expected have access to and comply with the most recent version of these security requirements.

7.3.4.2.6 RSU Interfaces

7.3.4.2.6.1 Interface between RSU and TMS

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

7.3.4.2.6.1.1 General RSU-TMS Interface Design Details

The design details to fulfill the general requirements for the security of data exchanges between an RSU and a TMS follow.

SNMPv3 is an application layer protocol that runs on top of security protocols like TLS or SSH.

7.3.4.2.6.1.1.1 Secure Transport of Use of SNMPv3

When using SNMPv3, the RSU shall use the Transport Layer Security Transport Model, as defined by RFC 6353 or later.

NOTE: RFC 6353 is based on (D)TLS 1.2 and there are technical ambiguities as to how it should be paired with (D)TLS 1.3. While RFC 6353 is expected to be updated to address these issues, RSU implementations prior to the release of this update are allowed to use (D)TLS 1.2 for SNMPv3 operations.

The RSU shall comply with CTI 4001, 4.3.5.11.1.1, Secure Administration - SNMPv3 Design Details.

7.3.4.2.6.1.1.2 Use of (D)TLS for other Management Protocols

The RSU shall use TLS 1.3 as specified in CTI 4001, 4.3.5.2, Local and Back-Office Interface Security Design Details, for interfaces implementing HTTPS or WebSocket protocols when the RSU is acting as a TLS server. For example, this would apply to a REST API implemented by the RSU.

The RSU may also support DTLS 1.3.

The RSU shall not implement unsecured communication using HTTP.

7.3.4.2.6.1.1.3 Use of SSH

The RSU shall implement SSH 2.0 as specified in RFC 4253.

NOTE: In order to fully support NTCIP 1218, the RSU has to implement SFTP (or SCP) as a mechanism to transfer files to and from the RSU. SFTP and SCP both use SSH 2.0 as the underlying secure transport protocol.

The RSU may limit SSH 2.0 protocol access to SFTP (or SCP) only and prevent remote command line access via SSH.

The RSU shall comply with CTI 4001, 4.3.5.11.1.3, Secure Administration - SSH Design Details.

7.3.4.2.6.1.2 (D)TLS Certificate Design Details

The design details to fulfill the requirements for TLS and DTLS certificates (X.509 format) for an RSU follow.

7.3.4.2.6.1.2.1 (D)TLS Authentication - Installation

If the RSU acts as a TLS or DTLS server, the RSU shall support installation of a chain of trust for validation of client certificates via a secure, vendor-specific mechanism, as defined in CTI 4001, 4.3.5.12.1, Secure Interface for X.509 Credentials for TLS Design Details. For additional information, see 0, 7.3.4.2.6.1.2.3RSU Certificate Security.

If the RSU acts as a TLS or DTLS server, the RSU shall support installation or configuration of an IOO-specific naming pattern for certificates (see 0).

7.3.4.2.6.1.2.2 (D)TLS Authentication - Rejection

When the RSU acts as a TLS or DTLS server, the RSU is required to reject connection attempts from clients presenting an invalid client certificate.

To do so, the RSU currently validates a client's certificate based on the following minimum criteria:

a. The current date is within the client certificate's validity time period.

b. The client certificate has been signed by a CA, which is listed as part of an installed chain of trust.

c. The client certificate is contained within the certificate "allow list" (as indicated in CTI 4001, 4.3.5.9.1, Assurance of Correct Initial Network Connection Design Details, and 4.3.5.9.2, Assurance of Continued Correct Network Connection Design Details).

However, the "allow-list" does not accommodate the frequently changing nature of client certificates. Therefore, the allow-list provision is deprecated (not recommended for new implementations). New implementations should use, and existing implementations should migrate to, a SubjectAltName design provision, as follows:

- Replacement c) provision: The SubjectAltName field in the client certificate matches an IOO-specific naming pattern (e.g., to distinguish between certs from the same root certificate authority but for different IOOs). The naming pattern shall support wildcards which can be used to allow all names with a certain suffix, e.g., "*.cityofnyc.gov."

NOTE 1: The alternate design using SubjectAltName and naming pattern is preferred, and the "allow list" practice is deprecated and efforts are underway to incorporate this change in CTI 4001.

NOTE 2: "Allow-lists" still exist for CA certificates by virtue of the CA certificates being part of a chain of trust. However, CA certificates roll over much less frequently.

7.3.4.2.6.1.2.3 RSU Certificate Security

If the RSU acts as a TLS or DTLS server, the RSU shall support installation of a private key and corresponding certificate containing the public key by an administrator. The RSU shall use the key and corresponding certificate to identify the server to CI components it connects to.

The RSU server certificate shall have the X.509 standard format and shall be signed by a certificate authority (CA) trusted by the IOO.

NOTE: The IOO may use a commercial CA service or operate its own public key infrastructure.

The RSU shall support installation of at least one chain of trust, containing at least one trusted CA certificate, by an administrator. A chain of trust may also contain one or more intermediate CA certificates and a trust anchor certificate (aka root certificate). In the chain of trust, the lowest CA's certificate has been signed by the next higher CA, chaining all the way to the top CA, also known as the root CA.

If the RSU acts as a TLS or DTLS server, the RSU shall use the methods of 0, 7.3.4.2.6.1.2.2(D)TLS Authentication - Rejection, to validate client certificates.

If the RSU acts as a TLS or DTLS client, the RSU shall use this chain of trust to validate server certificates of TLS servers that it connects to.

7.3.4.2.6.1.2.4 RSU Client Certificate Security

The RSU shall support the configuration of a SubjectAltName pattern which is used to validate TLS client certificates (see also 0, 7.3.4.2.6.1.2.2(D)TLS Authentication - Rejection).

The IOO shall have assurance that the SubjectAltName entries in each of their issued certificates are unique under the CA that issued the certificates.

The RSU shall provide an interface to allow an administrator to install trust anchors for X.509 certificates.

The RSU shall support trust anchor installation by one or more of the following methods and shall not support other methods for installing trust anchors:

a. A logged in administrator, using an administrator password, installing the trust anchor interactively (see NOTE 1)

b. An authenticated SNMPv3 operation

c. An automated operation involving signatures that chain back to an existing trust anchor.

d. Via an authenticated operation using (D)TLS 1.3 with a protocol other than SNMPv3, e.g., HTTPS (i.e., REST API) or WebSocket

NOTE 1: (a) May only be used to install an initial chain of trust, when no other is installed. After that, method (b), (c), or (d) must be used, i.e., a (D)TLS-protected protocol is used to update.

NOTE 2: The above requirements are due to the fact that installation of trust anchors is a very sensitive operation. These requirements are expected to be updated in future versions of this document and deployments may need to adhere to these new requirements in order to continue to be issued new certificates.

NOTE 3: RSU (D)TLS server certificates as well as (D)TLS client certificates are expected to be relatively short-lived, having a validity period on the order of one week or two. With this approach, it is possible to omit usage of CRLs and/or Online Certificate Status Protocol (OCSP) calls to a CA server in order to check the revocation status of individual certificates while still achieving a reasonable level of security protection.

7.3.4.2.6.2 Interface between RSU and SCMS

The RSU shall comply with CTI 4001, 4.3.5.10.3.1, SCMS Connectivity Design - CAMP.

Alternatively (and preferred going forward for new implementations), the RSU shall comply with CTI 4001, 4.3.5.10.3.2, SCMS Connectivity Design – IEEE Std 1609.2.1.

The CI backend network shall require secure domain-name server lookup for IP addresses obtained from outside their network, i.e., DNSSEC (according to RFC 4033, 4034, and 4035).

7.3.4.2.6.3 Interface between an RSU and the OBU/MU

The RSU shall ensure that the messages it sends across the RSU to OBU interface are secured as follows:

- SPaT messages are signed as per IEEE Std 1609.2 and the SPaT security profile of CTI 4501/1, Annex B.1
- MAP messages are signed as per IEEE Std 1609.2 and the MAP security profile of CTI 4501/2, Annex A.1
- RTCMcorrections messages are signed as per IEEE Std 1609.2 and the RTCMcorrections security profile in SAE J3258, Appendix C.

SPaT messages may be signed by the RSU. MAP messages may be signed by the MAP data server. RTCMcorrections messages may be signed by the RSU or the RTCM source.

The RSU shall comply with CTI 4001, 4.3.5.1.1, Security - Sending V2X Messages Design Details.

The RSU shall comply with CTI 4001, 4.3.5.1.2, Security - Receiving and Forwarding V2X Messages Design Details.

NOTE: If a message for transmission by the RSU is signed in a different location, then to comply with this design detail, the RSU will carry out the following checks:

- On reception of the message: fully validate that the message is validly signed per IEEE Std 1609.2 and the relevant security profile.
- On reception of any CRL or CTL: ensure that all certificates relied on for trust of the message are still trusted, i.e., no certificates in the chain have been revoked and the root certificate is still on the relevant CTL.
- If the signing certificate expires: stop retransmitting the message.

7.3.4.2.6.4 Interface between an RSU and the TSC Infrastructure

The design details to fulfill the requirements for the security of data exchanges between an RSU and a TSC infrastructure follow. These requirements are defined in 6.3.4.4.

7.3.4.2.6.4.1 Use of Secure Transport Protocol

The RSU shall implement the NTCIP 1202 v03 interface as specified in CTI 4001, 4.3.2.14.2, SPaT Processing Design Details - NTCIP 1202.

The RSU shall secure this interface, and any SNMPv3 interface, using SNMPv3 over TLS 1.3 or DTLS 1.3 (TLS 1.2 or DTLS 1.2 until version 1.3 is available for use with SNMP) with mutual authentication, with the RSU acting as a (D)TLS server.

The TSC infrastructure shall use this interface to establish a secure connection with the RSU and send SPaT information to the RSU.

7.3.4.2.6.4.2 Use of (D)TLS Protocol

The TSC infrastructure shall use its client certificate to authenticate itself to the RSU via SNMPv3 over TLS 1.2.

The TSC infrastructure shall support a vendor-specific and secure mechanism to install a client certificate along with a private key.

The TSC infrastructure shall support a vendor-specific and secure mechanism to install a chain of trust for validation of the RSU's (D)TLS server certificate.

The (D)TLS certificate design details specified in 0, 7.3.4.2.6.1.2(D)TLS Certificate Design Details, apply to the interface between the TSC infrastructure and the RSU.

7.3.4.2.6.4.3 Protection against TSC Infrastructure Reconfiguration from the RSU

The TSC infrastructure shall be protected against reconfiguration from the RSU by any vendor-specific means. This means shall be documented as part of the security documentation.

7.3.4.2.7 Interface between the TMS and the TSC Infrastructure

The communication on this interface shall be secured using mutual authentication of both TMS and TSC infrastructure identities and at least integrity protection of all data exchanged. It is preferred to use SNMPv3 over TLS or DTLS 1.3 or, if not yet available, over TLS or DTLS 1.2.

7.3.4.2.8 Interface between the MAP Server and the TMS

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

7.3.4.2.8.1 Secure Connection to MAP Server

A TMS shall establish a connection to the MAP server that supports transport layer security via the TLS 1.3 protocol, with certificate-based mutual authentication and integrity and encryption of data exchanged.

7.3.4.2.8.2 MAP Data Signature

The signature generated by the MAP server for the MAP message sent to the TMS shall follow the MAP message security profile in CTI 4501/2, Annex A.1, Security Profile for MAP Messages.

NOTE: The "generation time" is the time instance that the MAP message is signed.

7.3.4.2.9 Interface between MAP Server and the SCMS

The MAP server shall be able to periodically connect to a SCMS Registration Authority server configured in the MAP server in order to obtain IEEE Std 1609.2 certificates with appropriate permissions to sign MAP messages.

7.3.4.2.10 Credential Provisioning - (D)TLS Design Details

The design details to fulfill the requirements for provisioning a component of a connected intersection with TLS or DTLS client or server certificates follow.

7.3.4.2.10.1 Start-up Initialization

An RSU shall support the secure installation of (D)TLS signing certificates and of the (D)TLS Root (trust anchor) certificate(s) (and any intermediate CA certificates) as per CTI 4001, 4.3.5.12.1, Secure Interface for X.509 Credentials for TLS Design Details.

A TSC infrastructure shall support a secure installation of a (D)TLS signing certificate for itself. In addition, a TSC infrastructure shall support secure configuration of the (D)TLS Root Certificate Authority certificate to trust and optionally its allow-list of TLS end entities that the TSC infrastructure can trust.

A TMS can be initialized by any vendor-specific means.

A Map Data Server need not be initialized for TLS certificate use.

7.3.4.2.10.2 Credential Updates

An RSU shall support the update of (D)TLS certificates and the update of (D)TLS Root certificates (and any intermediate CA certificates) as per CTI 4001, 4.3.5.12.1, 4.3.5.12.2, and 4.3.5.12.3.

A TSC infrastructure should support a secure update of the (D)TLS certificates and the update of (D)TLS Root (trust anchor) certificates (and any intermediate CA certificates) to trust.

The TMS may keep track of the expiration time of RSU certificates and TSC infrastructure certificates and (even) that of the Map Server certificates.

A TMS shall support secure update of its (D)TLS certificates and the (D)TLS Root certificate(s). This update may be vendor-specific.

7.3.4.2.11 Management of Untrustworthy Devices - (D)TLS Design Details

The design details to fulfill the requirements for protecting the system from exchanging data with untrustworthy devices follow. These requirements are defined in 6.3.4.4.

7.3.4.2.11.1 Monitor Certificate Status

The certificates of the (D)TLS clients that the RSU TLS server connects to shall be monitored for validity, as detailed in 0, 7.3.4.2.6.1.2.2(D)TLS Authentication - Rejection.

7.3.4.2.11.2 Drop Connections

If an RSU or a TSC infrastructure element, while running or before setting up a TLS or other secure session, finds that the peer device does not have a valid certificate, then the RSU or TSC infrastructure shall immediately close the secure connection or drop the secure connection to that other peer device.

In addition, CTI 4001, 4.3.5.12.4, Expiration of Credentials Design Details, applies.

7.3.4.2.12 Credential System Access - SCMS Design Details

The design details to fulfill the requirements to support SCMS credentials follow. These requirements are defined in 6.3.4.4.

7.3.4.2.12.1 Connectivity Design

An RSU shall support a secure bootstrapping process at the beginning of its life cycle in order to be provisioned with initial SCMS trust material, as per CTI 4001, 4.3.5.10.1.1, SCMS Bootstrap Design Details.

An RSU shall support a secure enrollment process for SCMS, as per CTI 4001, 4.3.5.10.1.2, SCMS Enrollment Design Details - CAMP, or preferably CTI 4001, 4.3.5.10.1.3, SCMS Enrollment Design Details - IEEE Std 1609.2.1.

An RSU shall support connecting to an IOO-approved SCMS as per CTI 4001, 4.3.5.10.3.1, SCMS Connectivity Design Details - CAMP, or preferably CTI 4001, 4.3.5.10.3.2, SCMS Connectivity Design Details - IEEE Std 1609.2.1.

The MAP signer (i.e., the MAP Data Server component in charge of signing MAP messages) shall support a secure bootstrapping process at the beginning of its life cycle in order to be provisioned with initial SCMS trust material, similar to the CTI 4001, 4.3.5.10.1.1, SCMS Bootstrap Design Details.

The MAP signer shall support a secure enrollment process for SCMS, similar to the CTI 4001, 4.3.5.10.1.2, SCMS Enrollment Design Details - CAMP, or preferably CTI 4001, 4.3.5.10.1.3, SCMS Enrollment Design Details - IEEE Std 1609.2.1.

The MAP signer shall support connecting to an IOO-approved SCMS, similar to the CTI 4001, 4.3.5.10.3.1, SCMS Connectivity Design Details - CAMP, or preferably CTI 4001, 4.3.5.10.3.2 SCMS Connectivity Design Details - IEEE Std 1609.2.1.

NOTE: How to accommodate an off-site MAP signer is to be determined.

7.3.4.2.12.2 Download SCMS Files

The RSU shall download updated CRLs and SCMS files as in the CTI 4001, 4.3.5.10.6.1, Download SCMS Files Design Details - CAMP, or preferably CTI 4001, 4.3.5.10.6.2, Download SCMS Files Design - IEEE Std 1609.2.1.

Initially, the CAMP design can be supported, but longer term the IEEE Std 1609.2.1 shall be supported.

The RSU knows when to obtain a new CRL from the body of the current CRL file it has: the RSU should fetch an updated CRL "within a day of the time indicated by the next CRL field in the current CRL file."

An arrangement may be supported whereby new CRLs are downloaded by the TMS and then sent to the RSU.

NOTE: It may be assumed that, commonly, new CRLs may be issued approximately every week.

7.3.4.3 Trustworthiness of TSC-Originating Information: Design Details

The design details to fulfill the security requirements for trustworthiness of TSC-originating information for a connected intersection follow.

7.3.4.3.1 Trustworthiness of TSC-Originating Information: General

A connected intersection shall fulfill the requirements of 6.3.4.3 by the means specified in this section or by vendor-specific means in the case where this section does not give specific design details. The CI operator shall create documentation that documents how those requirements are met.

This documentation shall include at least the following:

- How the TSC Infrastructure is protected against modifications (via the expected update process, or via an attack, or via some other means) that would cause it to output incorrect information per 6.3.4.3.1, 6.3.4.3.2, 6.3.4.3.3, 6.3.4.3.4, 6.3.4.3.5.

Example 1: Protection against modifications via the expected update process could be accomplished as follows:

- Firmware and software updates shall be authenticated (e.g., digitally signed) by the TSC infrastructure element’s vendor and shall be installed only by a user with administrator privilege to the TSC element.

- Configuration parameters that affect SPaT content in such a way that the SPaT information might not reflect the actual state and timing of the TSC shall be changeable only by an administrator authorized to do so and over a secure connection after being authenticated.

Example 2: Protection against modifications via attacks could be accomplished by fulfilling the requirements of 6.3.4.1.

7.3.4.4 Approaching Vehicle Information Trustworthiness: RSU: Design Details

The design details to fulfill the security requirements for RSU approaching vehicle information trustworthiness for a connected intersection follow.

7.3.4.4.1 Approaching Vehicle Information Trustworthiness: RSU: General

A connected intersection shall fulfill the requirements of 6.3.4.4 by the means specified in this section or by vendor-specific means in the case where this section does not give specific design details. The CI operator shall create documentation that documents how those requirements are met.

This documentation shall include at least the following:

- Whether the RSU distinguishes between different BSM senders per 6.3.4.4.5.
- How the RSU is protected against modifications (via the expected update process, or via an attack, or via some other means) that would cause it not to comply with 6.3.4.4.6, 6.3.4.4.7.

Example 1: Protection against modifications via the expected update process could be accomplished as follows:

- Firmware and software updates shall be authenticated (e.g., digitally signed) by the RSU vendor and shall be installed only by a user with administrator privilege to the RSU.
- Configuration parameters that affect use of BSMs by the RSU shall be changeable only by an administrator authorized to do so and over a secure connection after being authenticated.

Example 2: Protection against modifications via attacks could be accomplished by fulfilling the requirements of 6.3.4.1.

7.3.4.4.2 1609.2 Validation of BSMs

An RSU shall validate received BSMs per IEEE Std 1609.2 and the IEEE Std 1609.2 Security Profile of SAE J3161/1 and SAE J2945/1 before processing those BSMs. Processing includes using information from the BSM about the sender's position in the intersection, forwarding the BSMs to other CI data entities, using for statistical purposes, and any other use.

7.3.4.4.3 Replay

An RSU shall use the generation time obtained from the BSM and the IEEE Std 1609.2 headerInfo, rather than the reception time, to determine the dynamics of the BSM sender. An RSU shall discard BSMs whose generation time is more than 30 seconds in the past, per the IEEE Std 1609.2 BSM security profile.

7.3.4.4.4 Misbehavior Detection

An RSU shall detect the BSM misbehaviors defined in SAE J3287 and may detect additional misbehaviors.

7.3.4.4.5 Misbehavior Reporting

An RSU may report the BSM misbehaviors defined in SAE J3287 to an appropriate Misbehavior Authority using the protocols defined in SAE J3287.

7.3.4.4.6 Misbehavior Reporting: Certificate

An RSU that generates misbehavior reports shall sign them with a certificate containing the Misbehavior Reporting PSID. This certificate shall be managed per the specifications of 7.3.4.2.

7.3.4.5 Approaching Vehicle Information Trustworthiness: TSC: Design Details

The design details to fulfill the security requirements for TSC approaching vehicle information trustworthiness and AGP for a connected intersection follow.

7.3.4.5.1 Approaching Vehicle Information Trustworthiness: TSC: General

A connected intersection shall fulfill the requirements of 6.3.4.5 by the means specified in this section or by vendor-specific means in the case where this section does not give specific design details. The CI operator shall create documentation that documents how those requirements are met.

This documentation shall include at least a statement of how the TSC protects against unnecessary AGP per 6.3.4.5.1.

7.3.4.5.2 Validation of Approaching Vehicle Information by TSC

For purposes of determining whether to apply an AGP, the TSC shall ignore all BSMs with a generation time more than 5 seconds in the past.

7.3.4.6 Time Source Trustworthiness: Design Details

The design details to fulfill the security requirements for time source trustworthiness and AGP for a connected intersection follow.

7.3.4.6.1 Time Source Trustworthiness: Design Details: General

A connected intersection shall fulfill the requirements of 6.3.4.6 by the means specified in this section or by vendor-specific means in the case where this section does not give specific design details. The CI operator shall create documentation that documents how those requirements are met.

This documentation shall include at least:

- An analysis of whether time sources can be delayed per 6.3.4.6.1
- A specification of how time source delay can be determined and mitigated per 6.3.4.6.2, 6.3.4.6.3, and 6.3.4.6.4
- A policy for when other users of external time sources shall be notified of observed delay per 6.3.4.6.5

7.3.4.7 SPaT Message Trustworthiness and Reliability: Design Details

The design details to fulfill the security requirements for SPaT message trustworthiness and reliability for a connected intersection follow.

7.3.4.7.1 SPaT Message Trustworthiness and Reliability: Design Details: General

A connected intersection shall fulfill the requirements of 6.3.4.7 by the means specified in this section or by vendor-specific means in the case where this section does not give specific design details. The CI operator shall create documentation that documents how those requirements are met.

This documentation shall include at least:

- The list of CI data entities that affect SPaT contents per 6.3.4.7.1
    - This list shall contain at least the RSU, the TSC infrastructure, and the systems at the TMS that are responsible for maintaining and configuring the RSU and the TSC Infrastructure.
- A statement that each of these CI data entities conforms to the relevant requirements of 6.3.4.1 per 7.3.4.1.
- A statement that for each logical data interface for each of those CI data entities that could affect SPaT correctness that logical data interface conforms to the relevant requirements of 6.3.4.2 per 7.3.4.2.

- A specification of how each of those CI data entities is protected against modification or attack that would lead to non-compliance with 6.3.4.7.2

- A specification of the mechanisms used to detect and manage inconsistency between SPaT data and actual signal times per 6.3.4.7.3, 6.3.4.7.4.

Example 1: Protection against modifications via the expected update process could be accomplished as follows:

- Firmware and software updates shall be authenticated (e.g., digitally signed) by the CI Data Entity vendor and shall be installed only by a user with administrator privilege.

- Configuration parameters that affect CI data shall be changeable only by an administrator authorized to do so and over a secure connection after being authenticated.

Example 2: Protection against modifications via attacks could be accomplished by fulfilling the requirements of 6.3.4.1.

7.3.4.7.2 SPaT Message Signing

The cryptographic keys used to sign the SPaT messages shall be protected from exposure per 6.3.4.2.24, 6.3.4.2.25, 6.3.4.2.26.

Example: This can be fulfilled by using NIST FIPS 140 Level 2 equivalent security and ensuring that only the process that creates the SPaT messages is allowed to request signing.

NOTE 1: This requirement is independent of the physical location in the architecture where SPaT signing takes place.

NOTE 2: The SCMS Provider may have specific requirements for protection of the keys that need to be met in addition to this design detail.

7.3.4.8 MAP Message Trustworthiness and Reliability: Design Details

The design details to fulfill the security requirements for MAP message contents trustworthiness for a connected intersection follow.

7.3.4.8.1 MAP Message Trustworthiness and Reliability: Design Details: General

A connected intersection shall fulfill the requirements of 6.3.4.8 by the means specified in this section or by vendor-specific means in the case where this section does not give specific design details. The CI operator shall create documentation that documents how those requirements are met.

This documentation shall include at least:

- The list of CI data entities that affect MAP contents per 6.3.4.8.1, 6.3.4.8.3

    - This list shall contain at least the RSU, the TSC infrastructure, and the systems at the TMS that are responsible for maintaining and configuring the RSU and the TSC Infrastructure.

- A statement that each of these CI data entities conforms to the relevant requirements of 6.3.4.1 per 7.3.4.1

- A statement that for each logical data interface for each of those CI data entities that could affect MAP correctness that logical data interface conforms to the relevant requirements of 6.3.4.2 per 7.3.4.2

- A specification of how each of those CI data entities is protected against modification or attack that would lead to non-compliance with 6.3.4.8.2

- A specification of the mechanisms used to detect and manage inconsistency between MAP data and road geometry or other real-world information per 6.3.4.8.4, 6.3.4.8.5, 6.3.4.8.6, 6.3.4.8.7

Example 1: Protection against modifications via the expected update process could be accomplished as follows:

- Firmware and software updates shall be authenticated (e.g., digitally signed) by the CI Data Entity vendor and shall be installed only by a user with administrator privilege.

- Configuration parameters that affect CI data shall be changeable only by an administrator authorized to do so and over a secure connection after being authenticated.

Example 2: Protection against modifications via attacks could be accomplished by fulfilling the requirements of 6.3.4.1.

7.3.4.9 RTCM Message Trustworthiness and Reliability: Design Details

The design details to fulfill the security requirements for RTCM message contents trustworthiness for a connected intersection follow.

7.3.4.9.1 RTCM Message Trustworthiness and Reliability: Design Details: General

A connected intersection shall fulfill the requirements of 6.3.4.9 by the means specified in this section or by vendor-specific means in the case where this section does not give specific design details. The CI operator shall create documentation that documents how those requirements are met.

This documentation shall include at least:

- The list of CI data entities that affect RTCM contents per 6.3.4.9.1, 6.3.4.9.3

- A statement that each of these CI data entities conforms to the relevant requirements of 6.3.4.1 per 7.3.4.1

- A statement that for each logical data interface for each of those CI data entities that could affect RTCM correctness that logical data interface conforms to the relevant requirements of 6.3.4.2 per 7.3.4.2

- A specification of how each of those CI data entities is protected against modification or attack that would lead to non-compliance with 6.3.4.9.2

Example 1: Protection against modifications via the expected update process could be accomplished as follows:

- Firmware and software updates shall be authenticated (e.g., digitally signed) by the CI Data Entity vendor and shall be installed only by a user with administrator privilege.

- Configuration parameters that affect CI data shall be changeable only by an administrator authorized to do so and over a secure connection after being authenticated.

Example 2: Protection against modifications via attacks could be accomplished by fulfilling the requirements of 6.3.4.1.

7.3.4.9.2 RTCM Corrections Data Trustworthiness

The (refer to SAE J2735) RTCM data can be obtained from the Network Transport of RTCM via Internet Protocol (NTRIP), from a Continuously Operating Reference Station (CORS), or from other sources of positioning corrections. The connected intersection shall ensure the trustworthiness of the source of this data by vendor-specific means and shall provide documentation how this requirement is met.

If the RTCM message is already signed by the source, then the RSU shall verify the RTCM message according to the IEEE 1609 RTCMcorrections security profile in SAE J3258, Appendix C, Security, before sending it on the V2X interface.

See 4.3.4.6.2.3.

7.3.4.10 Consistency between MAPs and SPaTs: Design Details

A connected intersection shall fulfill the requirements of 6.3.4.10 by vendor-specific means. The CI operator shall create documentation that documents how those requirements are met.

This documentation shall include a specification of the mechanisms used to ensure compliance with 6.3.4.10.1, 6.3.4.10.2.

7.3.4.11 Unavailability Indications: Design Details

The design details to fulfill the security requirements for unavailability indications for a connected intersection follow.

7.3.4.11.1 Unavailability Indications: Design Details: General

A connected intersection shall fulfill the requirements of 6.3.4.11 by the means specified in this section or by vendor-specific means in the case where this section does not give specific design details. The CI operator shall create documentation that documents how those requirements are met.

This documentation shall include at least:

- The list of CI data entities that affect the generation of unavailability indications per 6.3.4.9.1
- A specification of how each of those CI data entities is protected against modification or attack that would lead to non-compliance with 6.3.4.11.1, 6.3.4.11.2, 6.3.4.11.3, 6.3.4.11.4

7.3.4.12 Intersection Identifier Trustworthiness: Design Details

The design details to fulfill the security requirements for intersection identifier trustworthiness for a connected intersection follow.

7.3.4.12.1 Intersection Identifier Trustworthiness: Design Details: General

A connected intersection shall fulfill the requirements of 6.3.4.12 by the means specified in this section or by vendor-specific means in the case where this section does not give specific design details. The CI operator shall create documentation that documents how those requirements are met.

This documentation shall include at least:

- A specification of the mechanisms used to assign intersection identifiers per 6.3.4.12.1
- A specification of how the use of incorrect intersection identifiers is detected per 6.3.4.12.2
- Optionally:
    - A specification of how incorrect intersection identifiers are managed per 6.3.4.12.3
    - A specification of how duplicate use of intersection identifiers by external parties is detected and managed per 6.3.4.12.4, 6.3.4.12.5

7.3.4.13 System Management and Recovery: Design Details

The design details to fulfill the security requirements for system management and recovery for a connected intersection follow.

7.3.4.13.1 System Management and Recovery: Design Details: General

A connected intersection shall fulfill the requirements of 6.3.4.13 by the means specified in this section or by vendor-specific means in the case where this section does not give specific design details. The CI operator shall create documentation that documents how those requirements are met.

This documentation shall include a specification of how the requirements of 6.3.4.13.1, 6.3.4.13.2, 6.3.4.13.3, 6.3.4.13.4, 6.3.4.13.5, 6.3.4.13.6, 6.3.4.13.7, 6.3.4.13.8, 6.3.4.13.9, 6.3.4.13.10, 6.3.4.13.11, 6.3.4.13.12, 6.3.4.13.13, 6.3.4.13.14, and 6.3.4.13.15 are fulfilled.

7.3.4.13.2 CI Operation Security Practices

The security documentation shall document both the policies for the computer equipment and the human operators of that equipment. The policy shall include information on how personnel are trained for security operations and any audits or periodic reviews of policies and procedures that will be performed.

7.3.4.13.3 Security Against Cyberattack Design Details

The design details to fulfill the requirements for security against cyberattacks follow. These requirements are defined in 6.3.4.13.4.

7.3.4.13.3.1 Cyberattack Recovery Plan

A cyberattack recovery plan recognizes and incorporates the principles identified in the CIS Controls Implementation Guide for Industrial Control Systems. In addition, cyberattack recovery plans require frequent updates to ensure that the plan remains effective as new attacks are developed and launched.

A connected intersection shall fulfill requirement 6.3.4.13.4 via IOO-specific means based on principles outlined in the CIS Controls Implementation Guide for Industrial Control Systems, Control 10 - Data Recovery Capabilities and Control 19 - Incident Response and Management.

7.3.4.13.3.2 Cyberattack Robustness

To maintain robustness, a connected intersection (and/or its operators) requires continuous vulnerability management via provisions in the CIS Controls Implementation Guide for Industrial Control Systems.

A connected intersection shall fulfill requirement 6.3.4.13.4 via IOO-specific means based on principles outlined in the CIS Controls Implementation Guide for Industrial Control Systems, Control 3 - Continuous Vulnerability Management, Control 6 - Maintenance, Monitoring, and Analysis of Audit Logs, and Control 8 - Malware Defenses.

7.3.4.13.4 Network Monitoring Design

The RSU shall comply with CTI 4001, 4.3.5.13, Logging for General and Security Purposes Design Details. This section requires an RSU to log successful and unsuccessful log-on attempts.

7.3.4.13.4.1 Network Protection

A connected intersection system shall implement network monitoring with continuous vulnerability management according to requirements 6.3.4.13.12, 6.3.4.14.1, via IOO-specific means based on principles outlined in the CIS Controls Implementation Guide for Industrial Control Systems, Control, Control 11 - Secure Configurations for Network Devices such as Firewalls, Routers, and Switches, and Control 12 - Boundary Defense.

For example, the firewall policy should not accept incoming connections to the RSU from outside the network and only allow the RSU to initiate connections to SCMS domains in which it is of the SCMS it is enrolled in.

7.3.4.14 Support Systems and Functions: Design Details

The design details to fulfill the security requirements for support systems and functions for a connected intersection follow.

7.3.4.14.1 Support Systems and Functions: Design Details: General

A connected intersection shall fulfill the requirements of 6.3.4.14 by the means specified in this section or by vendor-specific means in the case where this section does not give specific design details. The CI operator shall create documentation that documents how those requirements are met.

This documentation shall include a specification of how the requirements of 6.3.4.14.1, 6.3.4.14.2, 6.3.4.14.3, 6.3.4.14.4, and 6.3.4.14.5 are fulfilled.

7.3.4.15 Updates and Update Planning: Design Details

The design details to fulfill the security requirements for updates and update planning for a connected intersection follow.

7.3.4.15.1 Updates and Update Planning: Design Details: General

A connected intersection shall fulfill the requirements of 6.3.4.15 by the means specified in this section or by vendor-specific means in the case where this section does not give specific design details. The CI operator shall create documentation that documents how those requirements are met.

This documentation shall include a specification of how the requirements of 6.3.4.15.1, 6.3.4.15.2, 6.3.4.15.3, 6.3.4.15.4, 6.3.4.15.5, 6.3.4.15.6, and 6.3.4.15.7 are fulfilled.

7.3.4.16 System Operational Modes, Accesses, and Status: Design Details

The design details to fulfill the security requirements for system operational modes, accesses, and status for a connected intersection follow.

7.3.4.16.1 System Operational Modes, Accesses, and Status: Design Details: General

A connected intersection shall fulfill the requirements of 6.3.4.16 by the means specified in this section or by vendor-specific means in the case where this section does not give specific design details. The CI operator shall create documentation that documents how those requirements are met.

This documentation shall include a specification of how the requirements of 6.3.4.16.1, 6.3.4.16.2, 6.3.4.16.3, 6.3.4.16.4, and 6.3.4.16.5 are fulfilled.

7.3.4.17 V2X Message Transmission: Design Details

The design details to fulfill the security requirements for V2X message transmission for a connected intersection follow.

7.3.4.17.1 V2X Message Transmission: Design Details: General

A connected intersection shall fulfill the requirements of 6.3.4.17 by the means specified in this section or by vendor-specific means in the case where this section does not give specific design details. The CI operator shall create documentation that documents how these requirements are met.

This documentation shall include at least:

- The list of CI data entities that affect RTCM contents per 6.3.4.9.1
- A specification of how each of those CI data entities is protected against modification or attack that would lead to non-compliance with 6.3.4.9.2
- A specification of the mechanisms used to detect and manage inconsistency between SPaT data and actual signal times per 6.3.4.7.3, 6.3.4.7.4

Example 1: Protection against modifications via the expected update process could be accomplished as follows:

- Firmware and software updates shall be authenticated (e.g., digitally signed) by the CI Data Entity vendor and shall be installed only by a user with administrator privilege.
- Configuration parameters that affect CI data shall be changeable only by an administrator authorized to do so and over a secure connection after being authenticated.

Example 2: Protection against modifications via attacks could be accomplished by fulfilling the requirements of 6.3.4.1.

7.3.4.18 Verification of Connected Intersection System Security Design Details

The design details to fulfill the requirements to provide verification of a connected intersection's compliance to system security requirements follow. These requirements are defined in 6.3.4.18.

7.3.4.18.1 Security Compliance Assessment

The verification that the security compliance assessment documentation is complete and correct shall be accomplished by self-declaration. The security compliance assessment documentation shall be as specified in the security design details sections above.

NOTE: These security documentation requirements are anticipated to change over time. While self-declaration is currently acceptable, the security compliance assessment documentation requirements themselves may change over time (for example, becoming more specific), and self-declaration may be replaced by a certification process involving an external party. As such, the IOO shall identify which version of CTI 4501 the security compliance assessment documentation conforms with. Doing so may mitigate deployment delays associated with compliance security assessment documentation that may not conform to later requirements. Annex B provides an example process of how an IOO may prepare its security compliance assessment documentation.

7.3.5 Operations and Maintenance Design Details

No additional design details.

8. CONNECTED INTERSECTION TESTING

This section presents a testing framework to verify that the CI system conforms to the security requirements of CTI 4501. This testing framework provides guidance on how to create a verification plan that tests V2X messages for a conformant CTI 4501 implementation. The purpose of a verification plan is to confirm that the implementation fulfills all the requirements defined for a connected intersection(s).

This section presents EXAMPLES of:

- Conformance Testing for CI Communications Security Verification

The reader is encouraged to read CTI 4501/4 before reading the remainder of this section.

8.1 Conformance Testing Areas

CTI 4501 conformance testing for CI Communications Security Verification can be characterized as:

- Describes the scope, testing activities, and test documentation to verify a connected intersection fulfills the CTI 4501 security requirements for the messages across the interface between an RSU and an OBU/MU are properly signed.

8.2 Requirements to Test Case Traceability Matrix (RTCTM)

An example requirements-to-test-case traceability matrix (RTCTM) to verify conformance to security requirements in CTI 4501 is provided in Table 2. The 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 category
- 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, their relationships among each other, and the importance of test document. Each requirement to be verified is traced to a verification (test) case, which then can be traced to the appropriate stage(s) in the verification (test) procedures. A verification case is a logical grouping of communications interface and performance requirements that are to be verified together.

The RTCTM provided in Table 2 identifies an initial list of example test cases to be performed for CTI 4501 conformance testing for security. 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 test cases in the RTCTM all must be successfully performed to claim conformance with CTI 4501.

The 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 a 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 Table 2 should be fulfilled to claim conformance to CTI 4501. The test cases referenced in Table 2 are examples of test cases. The test case details and activities may vary for each agency based on the agency's policies, test methodologies, and preferred test tools.

8.2.1 Communications Security Verification

Communications security verification for CTI 4501 consists of verifying that the V2X messages exchanged between the RSU and OBU fulfill all the requirements identified in the RTCTM for Security Verification (see Table 2).

Table 2 - RTCTM - communications security verification

FR ID	Functional Requirement	Test Case Identifier	Test Case Name	Verification Method	Mandatory
6.3.4.1.6	Authorized CI Data Entities	Security-Data-Capture-2	Security Data Capture 2 - Signatures and Profiles for Received Messages. See Table 5.		
6.3.4.1.7	Authenticated CI Data Entities	Security-Data-Capture-2	Security Data Capture 2 - Signatures and Profiles for Received Messages. See Table 5.		
6.3.4.2.2	Secure Communications for CI Data Logical Interfaces	Security-Data-Capture-2	Security Data Capture 2 - Signatures and Profiles for Received Messages. See Table 5.		
6.3.4.2.4	Secure Communications: Integrity of External CI Data Outbound Logical Interfaces	Security-Data-Capture-1	Security Data Capture 1 - Signatures and Profiles for Broadcasted Messages. See Table 4.		
6.3.4.2.5	Secure Communications: Replay Protection	Security-Data-Capture-1 Security-Data-Capture-2	Security Data Capture 1 - Signatures and Profiles for Broadcasted Messages. See Table 4. Security Data Capture 2 - Signatures and Profiles for Received Messages. See Table 5.		
6.3.4.2.9	Secure Communications: Authentication of External CI Data Logical Interfaces	Security-Data-Capture-2	Security Data Capture 1 - Signatures and Profiles for Broadcasted Messages. See Table 4.		
6.3.4.2.10	Secure Communications: Authentication of External CI Data Outbound Logical Interfaces	Security-Data-Capture-1	Security Data Capture 1 - Signatures and Profiles for Broadcasted Messages. See Table 4.		
6.3.4.4.1	Validate Security of Approaching Vehicle V2X Messages	Security-Data-Capture-2	Security Data Capture 1 - Signatures and Profiles for Broadcasted Messages. See Table 4.		

8.3 Planned Activities

A verification plan must describe the activities to verify that a system fulfills the requirement. In this context, the verification plan describes the activities 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.

Refer to 8.3 in CTI 4501/4 for information on verification plans.

8.3.1 CTI 4501 Conformance Testing by Stage - Security

Table 3 represents an example of when a subset of CTI 4501 conformance testing for communications security may be performed or repeated during the different stages of a connected intersection's life cycle.

Table 3 - Verification by stage - security

Stage	Test Scope
Certification	Complete at Component Testing
Component Testing	Complete process and awarding through recognized service
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	Perform the test cases for a subset of mandatory and selected requirements
Burn-in Testing	Perform the test cases for a subset of mandatory and selected requirements
Operations and Maintenance	Perform the test cases for a subset of mandatory and selected requirements after changes to firmware or hardware

8.3.2 Example Test Methodology - Security

This section contains example test cases to verify a subset of security requirements defined in this document.

8.3.2.1 CI Security Test Case - Broadcasted Messages

Table 4 - Example test case - security data capture 1

Test Case	
ID: Security-Data-Capture-1	Security Data Capture 1 - Signatures and Profiles for Broadcasted Messages
Purpose:	Verify the signatures and profiles for the SPaT, MAP, and RTCMcorrections data stream output from RSU are correct per IEEE Std 1609.2 and the security profiles in the appropriate guidance document (CTI 4501/1, CTI 4501/2, and SAE J3258, respectively).
Objective:	Verify system interface between an RSU and an OBU. The test case verifies that the SPaT, MAP, and RTCMcorrections messages broadcast from the RSU are signed as per IEEE Std 1609.2 and the corresponding security profile in the appropriate guidance document (CTI 4501/1, CTI 4501/2, and SAE J3258, respectively).
Inputs:	• SPaT messages are signed as per IEEE Std 1609.2 and the SPaT security profile in CTI 4501/1, Annex B.1. • MAP messages are signed as per IEEE Std 1609.2 and the MAP security profile in CTI 4501/2, Annex A.1 • RTCM messages are signed as per IEEE Std 1609.2 and the RTCM security profile in SAE J3258, Appendix C
Expected Outcome(s):	All signatures and security profiles are verified as correct, including: structure of data and valid value of data content.
Feature Pass/Fail Criteria:	All signatures and security profiles in each of the three messages are verified as correct. Fail: Any other outcome.
Preconditions:	The RSU has IEEE Std 1609.2 certificates and can sign messages or the messages are already signed when the RSU receives them from within the connected intersection (system).

8.3.2.2 CI Security Test Case - Received Messages

Table 5 - Example test case - security data capture 2

Test Case	
ID: TC-Security-Data-Capture-2	Security Data Capture 2 - Signatures and Profiles for Received Messages
Purpose:	Verify the signatures and profiles for the BSM data stream received by the RSU are correct per IEEE Std 1609.2 and the security profiles in SAE J3161/1.
Objective:	Verify system interface between an RSU and an OBU. The test case verifies that the BSM messages received by the RSU are signed as per IEEE Std 1609.2 and the appropriate security profile in SAE J3161/1.
Inputs:	BSM messages are signed as per IEEE Std 1609.2 and the BSM security profile in SAE J3161/1.
Expected Outcome(s):	The message is verified as validly signed per IEEE Std 1609.2 and the appropriate security profile.
Feature Pass/Fail Criteria:	The message is verified as validly signed. Fail: Any other outcome.
Preconditions:	The RSU is up to date with trust management information (CRLs, CTLs, etc.).

Certification agencies and SCMS providers may have examples of verification methodologies and procedures to verify signatures and security profiles.

8.3.3 Test Environment

A verification plan needs to describe the test environment to provide a basis for comprehensive and consistent testing. Refer to CTI 4501/4, 8.3.5, Test Environment for an example on how to describe the test environment.

8.4 Test Documentation

Refer to CTI 4501/4, 8.4, Test Documentation for a description of the different types of test documentation that should be developed for testing and validation.

9. NOTES

9.1 Revision Indicator

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

PREPARED BY SAE CONNECTED TRANSPORTATION INTEROPERABILITY COMMITTEE

ANNEX A - SECURITY PROFILES [NORMATIVE]

This annex shows the IEEE Std 1609.2 security profiles and related material for the various V2X messages sent from the RSU to the OBUs: SPaT, MAP, and RTCMcorrections.

An implementation, such as an RSU, may have a separate security certificate for each security profile (i.e., have separate security certificate for each message) or may have a security certificate that contains security profile for more than one V2X message or V2X application.

A.1 SECURITY PROFILE FOR SPAT MESSAGES

Refer to CTI 4501/1, Annex B.1.

A.2 SECURITY PROFILE FOR MAP MESSAGES

Refer to CTI 4501/2, Annex A.1.

A.3 SECURITY PROFILE FOR RTCMCORRECTIONS MESSAGES

Refer to SAE J3258, Appendix C.

ANNEX B - SECURITY DOCUMENTS

This annex contains a series of example documents that are to be completed by an IOO to help assess if a CI implementation fulfills the security requirements and satisfies the security user needs defined in CTI 4501.

B.1 SECURITY DOCUMENT SD-1: LIST OF CI DATA ENTITIES AND INTERFACES

B.1.1 Introduction

The SD-1 document is a reference sheet used to organize the other documents in this series. It lists all the CI data entities as defined in Figure of 6.3.4.1 (or groups of multiple data entities as defined in 6.3.4.1.5) in the system and gives each a reference ID. The security analysis for each of the data entities is given in separate documents indexed by those reference IDs. These separate documents are all instances of “CTI 4501 Security Document SD-2” and are referred to below as “SD-2s.”

B.1.2 Instructions - SD-1 Document

The tables below comprise Security Document - 1 (SD-1) and are intended to be editable.

- Table 1.1 contains administrative information and should be edited by providing information in the second column corresponding to the topics in the first column.
- Table 1.2 is a list of the CI data entities and should be extended as necessary so there is one row per CI data entity (or group of entities).
- Table 1.3 is a list of the logical interfaces within the CI system and should be extended as necessary so there is one row per logical interface.

For SD-1, the person or people responsible for filling out this form correctly is referred to as the “documentation team.” Tasks that result in information being recorded in this document are referred to as if the documentation team is directly responsible for carrying them out because that makes this document easier to write. In practice, other parties may be responsible for the activity while the documentation team simply records it correctly.

For example, note 5 in B.2.7 below says “The reference ID … is assigned by the documentation team,” but the reference ID may be assigned by some other party if this makes sense administratively. In general, “X is done by the documentation team” may be read as “X is done by the documentation team or by some other appropriate actor inside or, if appropriate, outside the Connected Intersection organization.”

This document is presented as a Word template, but it may be more appropriate to generate it from a database rather than by manually filling in the Word template, because the information appears in multiple documents and generating the docs automatically may help reduce errors.

The “Organization Name” in Table 1.1 should be an official name for the road operator deploying the connected intersection or for an organization within that road operator if that makes sense (for example, if the “road operator” is an organization spanning many sites which are operated somewhat independently from each other). The organization name should be unique within North America.

The format for the change history in Table 1.1 is up to the documentation team.

The reference ID for each CI data entity is assigned by the documentation team. Each reference ID needs to be unique within the organization identified by Table 1.1. The documentation team has responsibility for ensuring uniqueness.

It is conceivable that within an organization, there will be different CI deployment projects with different documentation teams. In this case, the organization should ensure uniqueness of IDs assigned by different documentation teams. For example, the organization could assign an ID prefix and separator to each deployment project (such as “DP1:”).

With Table 1.2, the Data Entity Name is optional and is intended to be suitable to be used conversationally.

The Data Entity Description should be clear enough to allow a third party, who is familiar with CI systems in general but not with this specific deployment, to work out what physical/logical component is being referred to.

“Internal” CI data entities and “External” data entities are as defined in 6.3.4.1.1 and 6.3.4.1.5, respectively.

The logical interfaces associated with each CI data entity, listed in Table 1.3, are also listed in the SD-2 document associated with that data entity. Their inclusion in this document is recommended so that there is one document that contains the full inventory of data entities and logical interfaces, but Table 1.3 may optionally be omitted. If Table 1.3 is included, it might make sense for it to be automatically generated to reduce the risk of synch issues between this document and the SD-2 documents.

Security Document - 1 (SD-1)

Table 1.1 - Administration (SD-1)

Name of organization	
Contact details for person responsible for this document	
Date of this document	
Change history	

Table 1.2 - List of CI data entities

Entity Reference ID	Data Entity Name	Data Entity Description	Internal or external
(add rows as required)			

CTI 4501 reference: 6.3.4.1

Table 1.3 - List of CI data logical interfaces

Interface Reference ID	Reference IDs of entities communicating across interface	Interface Description	Internal or external
(add rows as required)			

CTI 4501 reference: 6.3.4.2.1

B.2 SECURITY DOCUMENT SD-2: SECURITY REQUIREMENTS FOR INDIVIDUAL INTERNAL CI DATA ENTITY LIST OF CI DATA ENTITIES AND INTERFACES

B.2.1 Introduction

The SD-2 document is a record of the security requirements met by an individual CI data entity as defined in CTI 4501, 6.3.4.1 (or groups of multiple data entities as defined in 6.3.4.1.5). An SD-2 should be completed for each CI data entity. The SD-1 document lists all the CI data entities that comprise a connected intersection - each CI data entity should be included in the SD-1 document.

B.2.2 Instructions - SD-2 Document

The tables below comprise Security Document - 2 (SD-2) and are intended to be editable.

- Table 2.1 contains administrative information and should be edited by providing information in the second column corresponding to the topics in the first column.
- Table 2.2 contains characteristics of the individual CI data entity.
- Table 2.3 is a list of the logical interfaces of the CI data entity and should be extended as necessary so there is one row per logical interface.
- Table 2.4 documents how the CI data entity meets the security requirements.

SD-2 is intended for use to define internal CI data entities, although it can also be to record information about external CI data entities if necessary.

B.2.3 Table 2.1 Administration

The documentation team (as described in B.1.2) is expected to fill in the second column.

B.2.4 Table 2.2 Characteristics

The documentation team is expected to fill in the third column.

Entries are free text unless indicated otherwise. For some entries (e.g., the various types of CI data) there may not be anything to fill in, in which case “n/a” or “none” is fine.

B.2.5 Table 2.3 List of CI Data Logical Interfaces Associated with the CI Data Entity

The documentation team is expected to fill in the entire table, adding rows as required.

The second column contains the Entity Reference ID of the CI data entity the subject CI Data Entity (as identified in Table 2.1) is communicating with across this interface.

B.2.6 Table 2.4 Security Requirements

The documentation team is expected to fill in the Support and Notes columns.

The values for the Conformance column are:

- O for optional
- C for conditional
- M for mandatory

The Conformance column allows the documentation team to succinctly record whether or not the requirement is met. C means that the item is mandatory if specific conditions are met. Refer to the notes in B.2.7, which point to requirements for the description of those conditions. All Mandatory items, and all Conditional items for which the conditions are met, must have a Y in the status column for the CI data entity to be conformant. Conditional and Optional items are light-gray highlighted in the table below to make them easier to spot.

The Notes column allows the documentation team to provide additional information. The format of information in the Notes column is up to the documentation team, but it should provide a brief description of how the requirement is met such that a reviewer can have some assurance that the requirement was at least understood. If an item is not satisfied (which can be the case for a conformant data entity if the item is optional or if the item is conditional and the condition is not met), the notes may be used to describe why it was considered not necessary to meet the requirement (although this is up to the documentation team).

B.2.7 Notes - SD-2

1. In this document, the person or people responsible for filling out this form correctly is referred to as the “documentation team.” Tasks that result in information being recorded in this document are referred to as if the documentation team is directly responsible for carrying them out because that makes this document easier to write. In practice, other parties may be responsible for the activity while the documentation team simply records it correctly. For example, note 0 below says “The reference ID … is assigned by the documentation team,” but the reference ID may be assigned by some other party if this makes sense administratively. In general, “X is done by the documentation team” may be read as “X is done by the documentation team or by some other appropriate actor inside or, if appropriate, outside the Connected Intersection organization.”

2. This document is presented as a Word template, but it may be more appropriate to generate it from a database rather than by manually filling in the Word template, because the information appears in multiple documents and generating the docs automatically may help reduce errors.

3. The “Organization Name” in Table 1.1 should be an official name for the road operator deploying the connected intersection or for an organization within that road operator if that makes sense (for example, if the “road operator” is an organization spanning many sites which are operated somewhat independently from each other). The organization name should be unique within North America.

4. The format for the change history in Table 1.1 is up to the documentation team.

5. The reference ID for each CI data entity is assigned by the documentation team. See further discussion in document SD-1.

6. “Internal” and “External” are as defined in 6.3.4.1.1 and 6.3.4.1.5.

7. The logical interfaces listed in Table 2.3 are also listed in Table 1.3 in the SD-1 document. It might make sense for Table 2.3 to be automatically generated to reduce the risk of synch issues between the SD-1 and the SD-2 documents.

8. Table 2.4, rows 1 and 2: This can be satisfied by saying something like “the entity uses TLS 1.3 for all connections and implements passwords for individual user authentication following the organizational policy.”

9. Table 2.4, rows 3 and 4: Like with rows 1 and 2, this can be satisfied by saying something like “the entity uses TLS 1.3 for all connections and implements passwords for individual user authentication following the organizational policy.”

10. Table 2.4, row 5: Examples of mechanisms to protect the integrity of operations are given in 6.3.4.1.8.

11. Table 2.4, row 6: This protection may be provided by mechanisms on the data entity or by mechanisms elsewhere in the system that limit the ability of other actors in the system to change the operating mode of the data entity. See 6.3.4.1.9 for references to definitions of the different operating modes.

12. Table 2.4, row 7: This requires the documentation team to have considered how the CI data entity updates its indication of the operating mode and to have identified risks that might cause it to indicate its operating mode incorrectly.

13. Table 2.4, row 8 and 9: These conditional requirements are mandatory if physical access to the data entity is under the control of the CI operators and do not apply otherwise. Whether or not this condition applies is based on the information recorded in Table 2.2, row 8.

14. Table 2.4, row 12: The mitigations referred to in this row may be implemented on the CI data entity itself or elsewhere in the system. The important thing is that they exist.

15. Table 2.4, row 13: This requirement is conditional. First, if mitigations for bad data are included elsewhere in the system, this requirement need not be met (and the notes should note where the mitigation is implemented). Second, if it is believed that based on the cybersecurity and correct operations mechanisms in place, the chance of receiving bad data is negligible, this requirement need not be met (and the notes should note that the chance is believed to be negligible). If there are multiple data sources with different properties - some are mitigated on the data entity and/or some are mitigated elsewhere and/or some are believed to be negligible - then the notes should identify which data is handled in which way and the “Support” column should be “N.”

16. Table 2.4, row 15: In the notes column, list the operational roles relevant to CI operations that apply on this data entity and note how they are protected (this can be as simple as “User accounts protected by password and privileges managed by standard account management mechanisms”).

17. Table 2.4, row 16: This requirement is conditional. It is mandatory if the CI data entity allows manual entry of CI data and does not apply otherwise.

18. Table 2.4, row 17: The notes should record how long the list of accesses is kept for; CTI 4501 doesn’t give a minimum time.

19. Table 2.4, row 19: The notes should record, for each item in the list (i.e., the baseline list as given in the form plus any additional items identified by the documentation team), whether there is self-monitoring and, if there isn’t, if this is because the impact is not significant OR monitoring for that item occurs elsewhere OR some other reason.

20. Table 2.4, row 21: The notes should either list the mitigations used or refer to a document where those mitigations are documented.

21. Table 2.4, row 26: The notes should list the events that are logged or refer to a document that lists those events.

22. Table 2.4, row 28: The notes should list who (which roles/people/services as appropriate) has access to the logs.

23. Table 2.4, row 34: Different types of software/firmware updates may have different authentication mechanisms, such as code signing or installation by an authorized user. The notes column should note all updateable software/firmware and the authentication mechanism for each.

24. Table 2.4, row 36: This conditional entry is mandatory if the CI data entity sends V2X messages; not applicable otherwise.

25. Table 2.4, row 38: This conditional entry is mandatory if the CI data entity sends cryptographically protected CI data; not applicable otherwise. (It will in practice apply to almost all CI data entities.) The notes should contain a reference to the risk analysis described in 6.3.4.2.24.

Security Document - 2 (SD-2)

Table 2.1 - Administration (SD-2)

Name of organization (see Table 1.1)	
Entity Reference ID (see Table 1.2)	
Data Entity Name (see Table 1.2)	
Data Entity Description (see Table 1.2)	
Contact details for person responsible for this document	
Date of this document	
Change history	

Table 2.2 - Characteristics (SD-2)

#	Ref	Topic	Information
1	6.3.4.1.1	List/description of CI data that originates on the CI data entity	
2	6.3.4.1.1	List/description of CI data that is transformed by the CI data entity	
3	6.3.4.1.1	List/description of CI data that passes through the CI data entity and is not intended to be transformed by it	
4	6.3.4.1.1	List/description of CI data that is used by the CI data entity	
5	6.3.4.1.2, 6.3.4.1.3	Manual data source (yes/no)?	
6	6.3.4.1.4	Permitted data that may be entered manually	
7	6.3.4.1.11	Physical location	
8	6.3.4.1.11	Does the CI organization control physical access to the CI data entity?	
9	6.3.4.1.13	List networks that the entity has access to/from which the entity can be accessed	
10		List organizations that can supply updates	
11		Privacy-sensitive information available for storage or processing	

Table 2.3 - List of CI data logical interfaces

Interface Reference ID	Entity Reference IDs	Interface Description	Internal or external
(add rows as required)			

CTI 4501 reference: 6.3.4.2.1

Table 2.4 - Security requirements

#	FR ID	Statement	Conformance	Support (Y / N)	Notes
1	6.3.4.1.6	The CI data entity provides proof of authorization for all CI data that it could have created or modified	M		
2	6.3.4.1.6	The CI data entity checks the proof of authorization for all CI data that it makes use of	M		
3	6.3.4.1.7	The CI data entity provides proof of authentication for all CI data that it could have created or modified	M		
4	6.3.4.1.7	The CI data entity checks the proof of authentication for all CI data that it makes use of	M		
5	6.3.4.1.8	The CI data entity implements mechanisms to protect the integrity of operations	M		
6	6.3.4.1.9	The CI data entity is protected from operating in or transitioning to the wrong operational mode	M		
7	6.3.4.1.10	The CI data entity correctly indicates its current operating mode	M		
8	6.3.4.1.11	Physical access to the CI data entity is secured	C		
9	6.3.4.1.12	Physical access control is effective during error states	C		
10	6.3.4.1.13	Logical access to the CI data entity is secured	M		
11	6.3.4.1.14	Logical access to the CI data entity is secured during error states	M		
12	6.3.4.1.15	Mechanisms are in place to mitigate risks arising from unauthorized logical or physical access to the data entity	M		
13	6.3.4.1.15, 6.3.4.1.18	The data entity implements mechanisms to mitigate risks arising from incorrect data being received from internal or external CI data entities	C		
14	6.3.4.1.16	Physical (if applicable) and logical access to the CI data entity is controlled during all of the following: • Initial installation • Maintenance or degraded operations • System updates • Software/firmware updates • System outages • Removal/decommissioning • Performing security management • Entering or leaving a Maintenance Mode • Power outages • Recovery from disruption	M		
15	6.3.4.1.19	The CI data entity implements access privileges	M		
16	6.3.4.1.20	For each type of manually entered data, the CI data entity ensures that it can only be entered by particular accounts	C		
17	6.3.4.1.21	The CI data entity maintains, or provides means for a different CI data entity to maintain, a list of accesses	O		
18	6.3.4.1.22	The CI data entity detects attempts by unauthorized parties to generate or modify CI data	O		

#	FR ID	Statement	Conformance	Support (Y / N)	Notes
19	6.3.4.1.23, 6.3.4.1.24, 6.3.4.1.25	The CI data entity implements self-monitoring to detect significant impacts on CI data. The self-monitoring covers the items in the bulleted list below and any other items listed in the notes column, unless those items are covered by monitoring activities off the CI data entity or could not cause significant impacts. The baseline set of items is: • Loss of network connection • Loss of power to any individual components • Loss of input CI data • Loss of assurance that output data is being received • Loss of signing certificate validity (because of expiry, revocation, or other reasons) • Failures of integrity of operation (see 6.3.4.1.8) • Integrity or authentication failures on CI data communications • Integrity or authentication failures on software updates • Failed user authentications, including excessive numbers of failed authentication attempts • Access to - including modification or removal of - system and device logs (including who/what performed the access) • Attempts of operators to invoke or disable functions and services for which they are not authorized • Modification of user/operator access rights and authenticators • Excessive resource consumption events which may indicate a type of Denial-of-Service attack • Modification of the diagnostic system's configuration • Update of the CI data entity’s software or other configuration	M		
20	6.3.4.1.26	The self-monitoring system on the CI data entity is robust against spoofing and other cyberattacks	M		
21	6.3.4.1.27	The CI data entity implements mitigations to be used if any self-monitoring test detects an error causing a significant impact on CI data	M		
22	6.3.4.1.28	There is an error state recovery plan for the CI data entity	M		
23	6.3.4.1.29	Incorrect statements about whether the CI data entity has recovered from an error state can be detected and the correct status can be determined	M		
24	6.3.4.1.30	There is a means to validate the authorization of statements about whether a CI data entity has recovered from an error state	M		
25	6.3.4.1.31	The means for the CI to recover from an error state are not an attack vector	M		
26	6.3.4.1.32, 6.3.4.1.34	Significant events identified by self-monitoring are logged	M		
27	6.3.4.1.35	There is a specified process to identify when the logging of events associated with the CI should change, i.e., should add or remove events or information	M		
28	6.3.4.1.36, 6.3.4.1.37	Event logs associated with the CI data entity are made available to appropriate parties in a timely fashion	M		

#	FR ID	Statement	Conformance	Support (Y / N)	Notes
29	6.3.4.1.40, 6.3.4.1.41	For all CI data used by the CI data entity, there is an evaluation of the risk (likelihood and impact) that the data is unavailable and a mitigation plan if the risk warrants such a plan	M		
30	6.3.4.1.42, 6.3.4.1.43	For all CI data stored by the CI data entity, there is an evaluation of the risk (likelihood and impact) that the storage fails, leading to unavailability of that data, and a mitigation plan if the risk warrants such a plan	M		
31	6.3.4.1.44	The notes column lists all privacy-sensitive information available for storage or processing by the CI data entity (or provides a reference to such a list). This list may be “None.”	M		
32	6.3.4.1.45	For all privacy-sensitive information identified in the previous row, the CI data entity implements mechanisms to protect that information from being exposed	M		
33	6.3.4.1.46	The CI data entity implements mechanisms to ensure that software/firmware/configuration updates are obtained from an authorized source	M		
34	6.3.4.1.47	The CI data entity authenticates and verifies the integrity of all software/firmware updates	M		
34	6.3.4.1.48	The CI data entity ensures that all software/firmware updates are initiated by an authorized user	M		
34	6.3.4.1.49	The CI data entity validates the successful completion of all software/firmware updates	M		
35	6.3.4.1.50	The CI data entity correctly reports (i.e., cannot be tricked into incorrectly reporting) its software/firmware/configuration version status	M		
36	6.3.4.1.51	The CA data entity protects V2X radio parameters against modification that causes other requirements not to be met	C		
37	6.3.4.1.52	There is a threat analysis that identifies any significant threats against the CI data entity that are not addressed by the requirements in this document, and mitigations are provided for those threats	M		
38	6.3.4.2.24 6.3.4.2.25 6.3.4.2.26	For all keys that the CI data entity uses across CI logical interfaces, those keys are appropriately protected by hardware mechanisms and by access control	C		

B.3 SECURITY DOCUMENT SD-3: INTERFACEID-[ENTITYID]-[[ENTITYID]…]: SECURITY REQUIREMENTS FOR INDIVIDUAL CI LOGICAL INTERFACES

B.3.1 Introduction - SD-3 Document

B.3.2 Instructions - SD-3 Document

B.3.3 Table 3.1 Administration

The documentation team (as described in B.1.2) is expected to fill in the second column.

B.3.4 Table 3.2 Characteristics

The documentation team is expected to fill in the fourth column.

Entries are free text unless indicated otherwise. For some entries (e.g., the various types of CI data) there may not be anything to fill in, in which case “n/a” or “none” is fine.

B.3.5 Table 3.3 Security Requirements

The documentation team is expected to fill in the fifth and sixth columns.

The fourth column is:

- O for optional
- C for conditional
- M for mandatory

The Status column allows the documentation team to succinctly record whether or not the requirement is met. C means that the item is mandatory if specific conditions are met. Refer to the notes (which in turn will refer to CTI 4501) for the description of those conditions. All Mandatory items, and all Conditional items for which the conditions are met, must have a Y in the status column for the CI data entity to be conformant.

The Notes column allows the documentation team to provide additional information. The format of information in the Notes column is up to the documentation team, but it should provide a brief description of how the requirement is met such that a reviewer can have some assurance that the requirement was at least understood. If an item is not satisfied (which can be the case for a conformant data entity if the item is optional or if the item is conditional and the condition is not met), the notes may be used to describe why it was considered not necessary to meet the requirement (although this is up to the documentation team).

B.3.6 Notes - SD-3

1. In this document, the person or people responsible for filling out this form correctly is referred to as the “documentation team.” Tasks that result in information being recorded in this document are referred to as if the documentation team is directly responsible for carrying them out because that makes this document easier to write. In practice, other parties may be responsible for the activity while the documentation team simply records it correctly. For example, note 0 above says “The reference ID … is assigned by the documentation team,” but the reference ID may be assigned by some other party if this makes sense administratively. In general, “X is done by the documentation team” may be read as “X is done by the documentation team or by some other appropriate actor inside or, if appropriate, outside the Connected Intersection organization.”

2. This document is presented as a Word template, but it may be more appropriate to generate it from a database rather than by manually filling in the Word template, because the information appears in multiple documents and generating the docs automatically may help reduce errors.

3. The “Organization Name” in Table 1.1 should be an official name for the road operator deploying the connected intersection or for an organization within that road operator if that makes sense (for example, if the “road operator” is an organization spanning many sites which are operated somewhat independently from each other). The organization name should be unique within North America.

4. The format for the change history in Table 2.1 is up to the documentation team.

5. The Entity Reference ID for each CI data entity is assigned by the documentation team. See further discussion in document SD-1.

6. “Internal” and “External” are as defined in 6.3.4.1.1 and 6.3.4.1.5.

7. The logical interfaces listed in Table 2.3 are also listed in Table 1.3 in the SD-1 document. It might make sense for Table 2.3 to be automatically generated to reduce the risk of synch issues between this document and the SD-2 documents.

8. Table 3.3, rows 1 and 2: This can be satisfied by saying something like “the entity uses TLS 1.3 for all connections and implements passwords for individual user authentication following the organizational policy.”

9. Table 3.3, rows 3 and 4: Like with rows 1 and 2, this can be satisfied by saying something like “the entity uses TLS 1.3 for all connections and implements passwords for individual user authentication following the organizational policy.”

10. Table 3.3, row 5: Examples of mechanisms to protect the integrity of operations are given in 6.3.4.1.8.

11. Table 3.3, row 6: This protection may be provided by mechanisms on the data entity or by mechanisms elsewhere in the system that limit the ability of other actors in the system to change the operating mode of the data entity. See 6.3.4.1.9 for references to definitions of the different operating modes.

12. Table 3.3, row 7: This requires the documentation team to have considered how the CI data entity updates its indication of the operating mode and to have identified risks that might cause it to indicate its operating mode incorrectly.

13. Table 3.3, row 8 and 9: These conditional requirements are mandatory if physical access to the data entity is under the control of the CI operators and do not apply otherwise. Whether or not this condition applies is based on the information recorded in Table 2.2, row 8.

14. Table 3.3, row 12: The mitigations referred to in this row may be implemented on the CI data entity itself or elsewhere in the system. The important thing is that they exist.

15. Table 3.3, row 13: This requirement is conditional. First, if mitigations for bad data are included elsewhere in the system, this requirement need not be met (and the notes should note where the mitigation is implemented). Second, if it is believed that based on the cybersecurity and correct operations mechanisms in place, the chance of receiving bad data is negligible, this requirement need not be met (and the notes should note that the chance is believed to be negligible). If there are multiple data sources with different properties - some are mitigated on the data entity and/or some are mitigated elsewhere and/or some are believed to be negligible - then the notes should identify which data is handled in which way and the “Support” column should be “N.”

16. Table 3.3, row 15: In the notes column, list the operational roles relevant to CI operations that apply on this data entity and note how they are protected (this can be as simple as “User accounts protected by password and privileges managed by standard account management mechanisms”).

17. Table 3.3, row 16: This requirement is conditional. It is mandatory if the CI data entity allows manual entry of CI data and does not apply otherwise.

18. Table 3.3, row 17: The notes should record how long the list of accesses is kept for; CTI 4501 doesn’t give a minimum time.

19. Table 3.3, row 19: The notes should record, for each item in the list (i.e., the baseline list as given in the form plus any additional items identified by the documentation team), whether there is self-monitoring and, if there isn’t, if this is because the impact is not significant OR monitoring for that item occurs elsewhere OR some other reason.

20. Table 3.3, row 21: The notes should either list the mitigations used or refer to a document where those mitigations are documented.

21. Table 3.3, row 26: The notes should list the events that are logged or refer to a document that lists those events.

22. Table 3.3, row 28: The notes should list who (which roles/people/services as appropriate) have access to the logs.

23. Table 3.3, row 34: Different types of software/firmware updates may have different authentication mechanisms, such as code signing or installation by an authorized user. The notes column should note all updateable software/firmware and the authentication mechanism for each.

24. Table 3.3, row 36: This conditional entry is mandatory if the CI data entity sends V2X messages; not applicable otherwise.

25. Table 3.3, row 38: This conditional entry is mandatory if the CI data entity sends cryptographically protected CI data; not applicable otherwise. (It will in practice apply to almost all CI data entities.) The notes should contain a reference to the risk analysis described in 6.3.4.2.24.

Security Document - 3 (SD-3)

Table 3.1 - Administration (SD-3)

The documentation team is expected to fill in the second column.

Name of organization (see Table 1.1)	
Interface Reference ID (see Table 2.3)	
List of Entity Reference IDs (see Table 2.3) for the CI data entities that communicate across this interface	
Interface Description (see Table 2.3)	
Contact details for person responsible for this document	
Date of this document	
Change history	

Table 3.2 - Characteristics (SD-3)

#	Ref	Topic	Information
1	6.3.4.2.2	Interface type: one of • Cryptographically protected logical interface • Physically protected interface • Interface with GNSS data source	
2	6.3.4.2.2	List/description of CI data that is passed across the interface	
3	6.3.4.2.2	Is interface between two internal CI data entities (write “internal”), or is one of the CI data entities external (write “external”)?	
3	6.3.4.2.19	List of privacy-sensitive information flows	

Table 3.3 - Security requirements (SD-3)

#	FR ID	Statement	Conformance	Support (Y / N)	Notes
1	6.3.4.1.6	The CI data entity provides proof of authorization for all CI data that it could have created or modified	M		
2	6.3.4.1.6	The CI data entity checks the proof of authorization for all CI data that it makes use of	M		
3	6.3.4.1.7	The CI data entity provides proof of authentication for all CI data that it could have created or modified	M		
4	6.3.4.1.7	The CI data entity checks the proof of authentication for all CI data that it makes use of	M		
5	6.3.4.1.8	The CI data entity implements mechanisms to protect the integrity of operations	M		
6	6.3.4.1.9	The CI data entity is protected from operating in or transitioning to the wrong operational mode	M		
7	6.3.4.1.10	The CI data entity correctly indicates its current operating mode	M		
8	6.3.4.1.11	Physical access to the CI data entity is secured	C		
9	6.3.4.1.12	Physical access control is effective during error states	C		
10	6.3.4.1.13	Logical access to the CI data entity is secured	M		
11	6.3.4.1.14	Logical access to the CI data entity is secured during error states	M		
12	6.3.4.1.15	Mechanisms are in place to mitigate risks arising from unauthorized logical or physical access to the data entity	M		
13	6.3.4.1.15, 6.3.4.1.18	The data entity implements mechanisms to mitigate risks arising from incorrect data being received from internal or external CI data entities	C		
14	6.3.4.1.16	Physical (if applicable) and logical access to the CI data entity is controlled during all of the following: • Initial installation • Maintenance or degraded operations • System updates • Software/firmware updates • System outages • Removal/decommissioning • Performing security management • Entering or leaving a Maintenance Mode • Power outages • Recovery from disruption	M		
15	6.3.4.1.19	The CI data entity implements access privileges	M		
16	6.3.4.1.20	For each type of manually entered data, the CI data entity ensures that it can only be entered by particular accounts	C		
17	6.3.4.1.21	The CI data entity maintains, or provides means for a different CI data entity to maintain, a list of accesses	O		
18	6.3.4.1.22	The CI data entity detects attempts by unauthorized parties to generate or modify CI data	O		

#	FR ID	Statement	Conformance	Support (Y / N)	Notes
19	6.3.4.1.23, 6.3.4.1.24, 6.3.4.1.25	The CI data entity implements self-monitoring to detect significant impacts on CI data. The self-monitoring covers the items in the bulleted list below and any other items listed in the notes column, unless those items are covered by monitoring activities off the CI data entity or could not cause significant impacts. The baseline set of items is: • Loss of network connection • Loss of power to any individual components • Loss of input CI data • Loss of assurance that output data is being received • Loss of signing certificate validity (because of expiry, revocation, or other reasons) • Failures of integrity of operation (see 6.3.4.1.8) • Integrity or authentication failures on CI data communications • Integrity or authentication failures on software updates • Failed user authentications, including excessive numbers of failed authentication attempts • Access to - including modification or removal of - system and device logs (including who/what performed the access) • Attempts of operators to invoke or disable functions and services for which they are not authorized • Modification of user/operator access rights and authenticators • Excessive resource consumption events which may indicate a type of Denial-of-Service attack • Modification of the diagnostic system's configuration • Update of the CI data entity’s software or other configuration	M		
20	6.3.4.1.26	The self-monitoring system on the CI data entity is robust against spoofing and other cyberattacks	M		
21	6.3.4.1.27	The CI data entity implements mitigations to be used if any self-monitoring test detects an error causing a significant impact on CI data	M		
22	6.3.4.1.28	There is an error state recovery plan for the CI data entity	M		
23	6.3.4.1.29	Incorrect statements about whether the CI data entity has recovered from an error state can be detected and the correct status can be determined	M		
24	6.3.4.1.30	There is a means to validate the authorization of statements about whether a CI data entity has recovered from an error state	M		
25	6.3.4.1.31	The means for the CI to recover from an error state are not an attack vector	M		
26	6.3.4.1.32, 6.3.4.1.34	Significant events identified by self-monitoring are logged	M		
27	6.3.4.1.35	There is a specified process to identify when the logging of events associated with the CI should change, i.e., should add or remove events or information	M		

#	FR ID	Statement	Conformance	Support (Y / N)	Notes
28	6.3.4.1.36, 6.3.4.1.37	Event logs associated with the CI data entity are made available to appropriate parties in a timely fashion	M		
29	6.3.4.1.40, 6.3.4.1.41	For all CI data used by the CI data entity, there is an evaluation of the risk (likelihood and impact) that the data is unavailable and a mitigation plan if the risk warrants such a plan	M		
30	6.3.4.1.42, 6.3.4.1.43	For all CI data stored by the CI data entity, there is an evaluation of the risk (likelihood and impact) that the storage fails, leading to unavailability of that data, and a mitigation plan if the risk warrants such a plan	M		
31	6.3.4.1.44	The notes column lists all privacy-sensitive information available for storage or processing by the CI data entity (or provides a reference to such a list). This list may be “None.”	M		
32	6.3.4.1.45	For all privacy-sensitive information identified in the previous row, the CI data entity implements mechanisms to protect that information from being exposed	M		
33	6.3.4.1.46	The CI data entity implements mechanisms to ensure that software/firmware/configuration updates are obtained from an authorized source	M		
34	6.3.4.1.47	The CI data entity authenticates and verifies the integrity of all software/firmware updates	M		
34	6.3.4.1.48	The CI data entity ensures that all software/firmware updates are initiated by an authorized user	M		
34	6.3.4.1.49	The CI data entity validates the successful completion of all software/firmware updates	M		
35	6.3.4.1.50	The CI data entity correctly reports (i.e., cannot be tricked into incorrectly reporting) its software/firmware/configuration version status	M		
36	6.3.4.1.51	The CA data entity protects V2X radio parameters against modification that causes other requirements not to be bet	C		
37	6.3.4.1.52	There is a threat analysis that identifies any significant threats against the CI data entity that are not addressed by the requirements in this document, and mitigations are provided for those threats	M		
38	6.3.4.2.24 6.3.4.2.25 6.3.4.2.26	For all keys that the CI data entity uses across CI logical interfaces, those keys are appropriately protected by hardware mechanisms and by access control.	C		

ANNEX C - ADDITIONAL INFORMATION - SECURITY [INFORMATIVE]

C.1 SECURING MESSAGES FROM SOURCE TO END RECIPIENT (EXAMPLE)

Let us say a communication system is such that a Message is produced by a device and is meant to be consumed by an end recipient. Message trustworthiness is paramount, and is achieved, in this scenario, by a (digital) signature that can be attached to the Message. Signatures have the benefit that if the Message or its signature is changed in any way, the recipient will be able to tell and so can discard that Message as untrustworthy. This is called "integrity protection."

For illustration sake, let us imagine a system where messages are produced and need to get delivered to a community of receivers, who can be assured of their trustworthiness. A trustworthy device, Alice, produces messages M. Another trustworthy device, Bob, gets messages from Alice and then sends them to a community of receivers. The communication channels between Alice, Bob, and the community may or may not be trusted; i.e., the channels may harbor attackers that can alter messages. In particular, the communication between Bob and the community of receivers is not secured. The receivers trust both Alice and Bob, i.e., can verify the signatures of either Alice or Bob on a given message, and that is sufficient to establish trustworthiness of the signed message. That is, recipients trust a message, M, if they can be assured that:

a. Alice produced it.

b. It hasn't been modified in its journey from Alice to them.

Let's look at two scenarios and go through the journey of a message M:

a. Alice produces the message and can sign it herself.

b. Alice produces the message but cannot sign it herself; only Bob can sign messages.

Scenario 1 is an illustration of the case of MAP messages, which get produced and signed by the MAP server and then distributed via the RSU for subsequent transmission to vehicles. Scenario 2 represents the case of SPAT messages, which get produced by the Traffic Signal controller, signed by the RSU, and then transmitted to vehicles.

We will show (informally) that a receiver can be assured a received message is trustworthy in both scenarios, with some conditions.

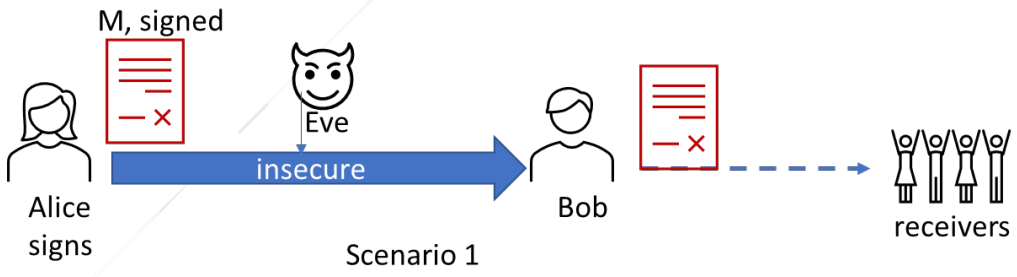

Figure C1 - Security scenario 1

Scenario 1: Since Alice is both the producer of the message and the signer of it, once a message M is signed, it has integrity protection which allows it to travel through untrustworthy channels and be passed via Bob or other devices, and the receivers can still verify that M was indeed produced by Alice and not altered. Thus, both (a) and (b) are easily satisfied by virtue of digital signatures applied at the source (Alice).

But can Scenario 2 be "just as good" as Scenario 1 in terms of assurance that the receiver can have?

Scenario 2 needs some expansion. Alice produces M, and since she can't sign it, she has to send it to Bob to sign. But if another device, Eve, gets between Alice and Bob, and intercepts this message and changes it from M to M', then Bob has no way to know. Bob will sign what he thinks Alice sent him, the changed message M'. Then after disseminating it to the community, the receivers will verify Bob's signature and wrongly assume that the M' they received is trustworthy.

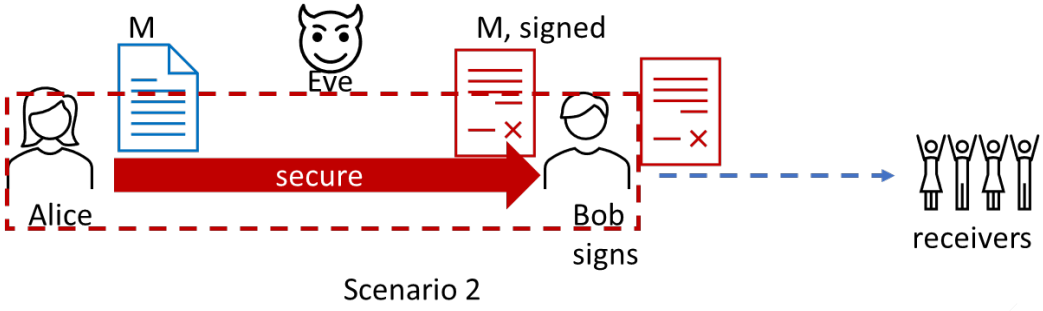

Figure C2 - Security scenario 2

In order to prevent this from happening, the communication channel between Alice and Bob must be secure in that no other device, Eve, can modify messages exchanged between them and go undetected. That is, if Bob can be assured that a message, M, he receives is exactly what Alice meant to send him, then Bob can go ahead and sign M and distribute it to the receivers; they will verify Bob's signature on Alice's message, and since they trust Bob and know that the message is truly the one Alice produced, they can be assured of both (a) and (b): of (a) because only Alice produces such content; and of (b) because the message was securely transferred between Alice and Bob, was signed by Bob, and sent to them via the (insecure) communication channel.

In Scenario 2, the secure channel between Alice and Bob allows us to view Alice and Bob as a team, as a single unit around which one can draw a "security boundary."

Our community of receivers can be assured that the messages they receive are trustworthy!

C.2 CERTIFICATION PROCESS

This section gives an overview of the Connected Intersection certification process. The elements involved are the following:

- IOO or Operating Agency. The IOO personnel (or process) responsible for the network security, where the network includes the Center and Field devices, and their interfaces. The IOO produces security compliance assessment documentation.

- Point of Certification (POC). An entity approved by the CI ecosystem that evaluates compliance assessments from IOOs in order to determine whether the CI network attains a certain level of security for a given set of aspects and formalize this result in a security certification.

  NOTE: For this version of this document, the POC is the IOO itself, and the certification is in effect a self-declaration.

- SCMS provider. An infrastructure-based security credential management system (SCMS) responsible for generating and delivering the IEEE Std 1609.2 security certificates that are used in the verification process of messages "between mobile elements and field infrastructure."

- (D)TLS certificate provider. An infrastructure-based credential management system responsible for generating and delivering the X.509 security certificates.

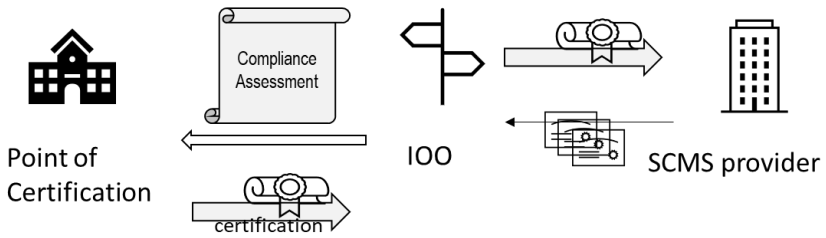

Figure C3 - CI certification ecosystem

The CI ecosystem is involved in selecting or designating POCs. A system may have multiple POCs.

The certifications that the POC produces are valid for a given amount of time (e.g., 1 year). The certification process is as follows:

1. The IOO assembles a security compliance assessment documentation. In the future, the IOO may employ third parties to perform security audits, penetration testing, or other such operations that result in attestation of the security posture of the network. This documentation is then provided to a designated POC.

2. The POC in turn evaluates the assessment and decides whether the IOO attains the security levels as expected. As a result, the POC returns to the IOO either a formal security certification or a result indicating further measures are to be employed and/or current measures adjusted. The IOO can then implement the additional measures and/or adjust the existing ones and produce updated compliance assessment documentation.

3. Once the IOO obtains a security certification from the POC, the IOO can submit it to a SCMS provider, who then is able to issue certificates to the devices (e.g., RSUs) or servers (e.g., MAP server) in the IOO network.

4. The IOO can follow step 3 for a TLS certificate provider.

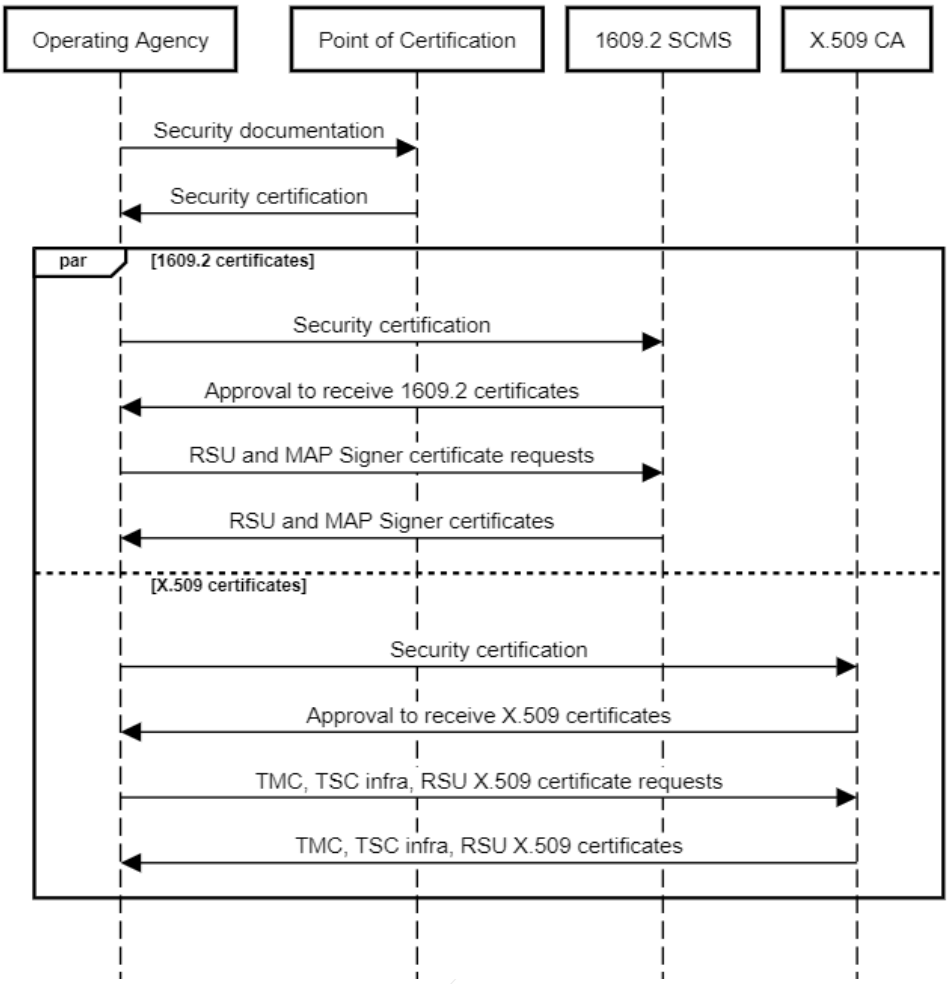

Figure C4 - CI certification process

C.3 ATTACK TREE EXAMPLES

C.3.1 Introduction

Attack trees and mitigations are part of the security compliance assessment documentation that an IOO can provide in order to show the security posture of their ITS deployment. This section provides a brief introduction to attack trees.

Attack trees are one of the oldest and most widely used methods to model threats, applicable to cyber-only systems, cyber-physical systems, and purely physical systems. At first, attack trees were applied as a stand-alone method, but over the years they have been used in conjunction with and as a helper to threat frameworks-based methodologies such as Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE) and MITRE ATT&CK® (Adversarial Tactics, Techniques and Common Knowledge).

Attack trees, also known as threat trees, were first introduced in 1999, and to this day they are still used in many systems to model adversarial threats and design respective mitigations. They are a tool to help enumerate the security threats an organization may face. The path that an adversary takes is described in a hierarchical or tree format: The root of the tree constitutes the overall goal of the attack, while the branch nodes indicate methods of achieving that goal. Each branch node represents an attack (action, event, activity), which in turn is the goal for the nodes beneath it, also referred to as child attacks. In summary, attack trees are a tool that helps with the tasks of threat brainstorming, adversary modeling, and mitigation development. An example of a simple attack tree is shown in Figure .

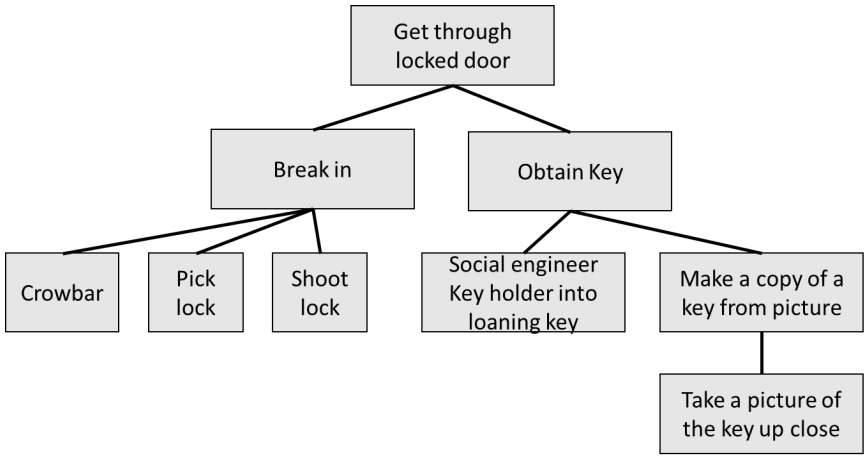

Figure C5 - Example of attack tree

C.3.2 Attack Tree Building Preliminaries

In the following sections, examples of attack trees will be shown for each use case (attack goal). Importantly, they are only ***examples*** for educational purposes; each IOO should construct their own based on their deployment. A tree diagram is also provided for illustrative purposes.

There are several attack trees that will be constructed, largely covering incorrect RSU outputs over the RSU-OBU interface. For the purposes herein, these are considered attacks, even though these events may also happen as a result of non-malicious misconfiguration or anomalous device behavior. The reason is if these misconfigurations or unintended behaviors are maliciously sourced, they may cause significant harm (e.g., to safety of vehicles using this information).

An attack tree may contain sub-trees, which are used to avoid a repetition of common attack tree segments (e.g., hacking the TMS or the MAP server require very similar steps). More basically, for each "parent" attack node in the attack tree, there are one or more actions that may or must take place in order to reach its goal, either independently (i.e., they are "disjunctive") or necessarily together (i.e., they are "conjunctive").

Each attack listed in the tree is to be accompanied by one or more mitigations that address that attack. Mitigations are measures that are expected to decrease the chance of an actual attack being successfully undertaken by an adversary; they are usually preemptive security controls, which are reasonable in terms of cost and continuous operation of the system. Mitigations can also be used to address the impact of a successful attack. If the risk from an attack (the combination of likelihood and impact) is believed to be sufficiently low, the mitigation can be recorded as "Attack is low risk, no mitigation required." The rules for mitigations recording are the following:

- All attacks must have recorded a mitigation or no need for mitigation.
- If an attack has child attacks, the mitigations should be specified at the level of the child attacks (this applies recursively). For example, a parent node mitigation includes "see child attack mitigations."
- This ensures that the complete mitigation for each identified attack can be identified without having to read "up the tree."
- This may result in duplicate mitigations being recorded in the tree: the duplicate mitigations can be combined into a single instance when the material from the tree is later used to create system requirements.
- Record the parent mitigation on each child attack even at the cost of duplication.
- If an attack does not have any child attacks, it must have a stand-alone mitigation recorded for it.
- On child attacks where the mitigation recorded for the parent attack fully mitigates the child attack too, one can record the mitigation as "See mitigation on parent."

It is important to note that a judgment call must be made about the level of detail to include in the attack tree. Including excessive detail makes the attack tree unwieldy, while omitting detail might lead to a threat not being covered that requires a specific mitigation, resulting in that mitigation not being implemented. Good guidance is that the attack tree should go to a level where the statement of the mitigation for an attack allows the attack to be completely mitigated - in other words, if there are child attacks that require significantly different mitigations from each other, the tree should be extended to explicitly capture those child attacks.

The following attack goals are in scope (from 6.3.4):

1. RSU outputs incorrect SPaT messages

2. RSU outputs incorrect MAP messages

3. RSU outputs incorrect positioning corrections (RTCMcorrections)

A SPaT, MAP, or RTCMcorrections message is considered "incorrect" if it fails to fulfill the requirements and design set forth in this document: for example, it does not match the actual traffic light signal from the TSC, does not fulfill applicable accuracy requirements, or it contains an invalid signature by the conditions of IEEE Std 1609.2 and its security profile.

C.3.3 Constructing an Attack Tree: RSU Outputs Incorrect SPaT Messages

An *example* attack tree showing some of the attacks that may cause an RSU to output incorrect SPaT messages is shown in Figure and is provided for illustrative purposes only. Such figures are optional to the IOO documentation. The attack tree can be described in list format, an example of which is shown next.

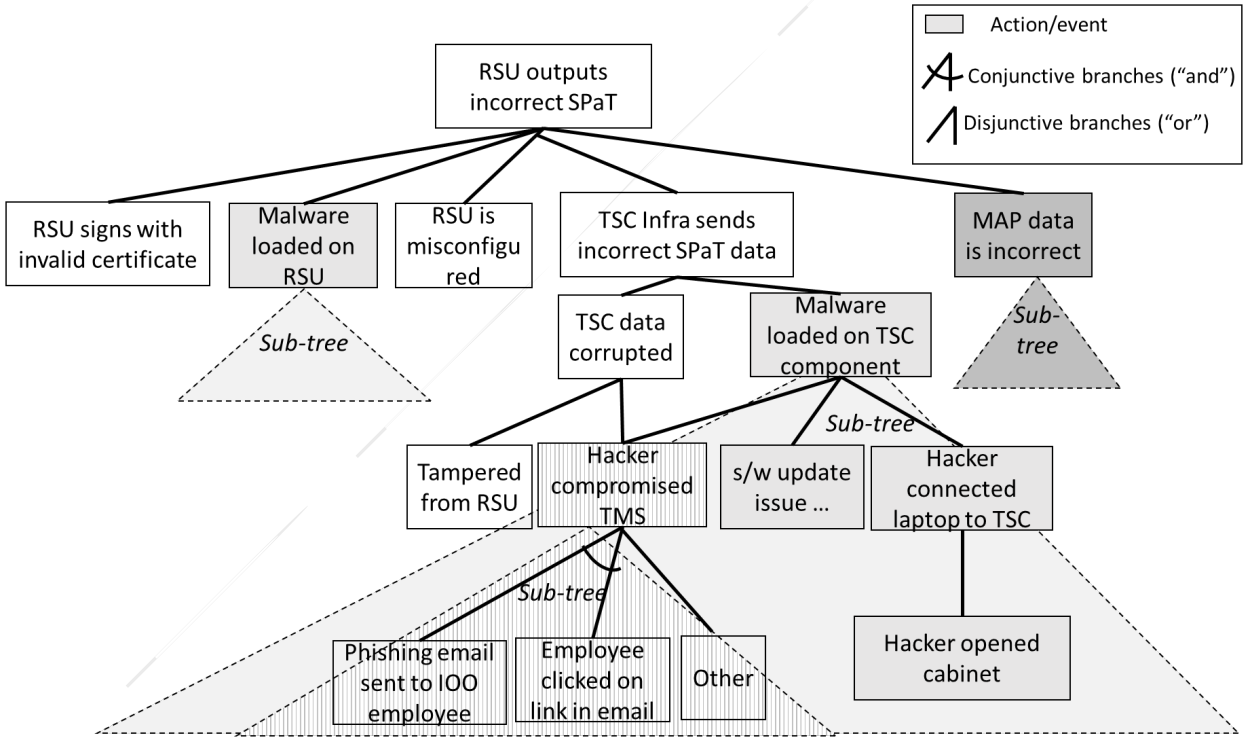

Figure C6 - Attack tree example - RSU outputs incorrect SPaT messages

"RSU outputs incorrect SPaT messages" attack tree

1. RSU outputs incorrect SPaT messages.

Possible actions that lead to this state are any of the following:

1.1 RSU signs with an invalid certificate. Possible actions that lead to this state are any of the following (not shown in the diagram):

1.1.1 RSU signs with an expired certificate. This may occur because the RSU's own certificate has expired or one in its chain has expired, and the RSU signing software does not check that the certificate is expired before signing.

1.1.2 RSU signs with a certificate with incorrect Provider Service Identifier (PSID). This may occur because the RSU's certificate has the incorrect PSID and the RSU signing software does not check that the certificate has the correct permissions before signing.

1.1.3 (Other attacks can be inserted here based on the ways in which a message can be inconsistent with the certificate as specified in *IEEE Std 1609.2* - for example, inconsistent SSP, inconsistent geographic region, etc. Alternatively, all the attacks that are mitigated by correct implementation of *IEEE Std 1609.2* will not be enumerated.)

1.2 Malware loaded on RSU causes incorrect SPaT messages to be constructed by the RSU. Possible actions that lead to this state are described in the "**Malware loaded on RSU**" sub-tree.

1.3 RSU is misconfigured. Possible actions that lead to this state are any of the following (not shown in the diagram):

1.3.1 RSU time source is caused to be out of sync. Possible actions that lead to this state are any of the following:

1.3.1.1 Attacker with logical access resets the clock.

1.3.1.2 Hardware error in clock chip leads to clock being out of sync with real time.

1.3.2 RSU is provided with incorrect map data to use to turn TSC information into SPaT lanes.

1.3.3 (other general misconfiguration actions or attacks)

1.4 TSC Infrastructure sends incorrect SPaT data to the RSU. Possible actions that lead to this state are:

1.4.1 TSC data is corrupted. Possible actions that lead to this state are:

1.4.1.1 Hacker compromised TMS. The hacker can use the TMS to spoof TSC data. Possible actions that lead to this state are described in the "**Hacker compromised TMS**" attack sub-tree.

1.4.1.2 TSC data is tampered with or spoofed in transit between TSC and the RSU. Possible actions that lead to this state are: hacker compromised a middlebox (router, switch) in the ITS network and is able to alter the data without detection due to lack of transport-layer security (TLS).

1.4.2 Malware loaded on the TSC infrastructure component. Possible actions that lead to this state are described in the "**Malware loaded on TSC**" sub-tree.

1.5 MAP data is incorrect, so the RSU makes an incorrect translation from TSC information to SPaT format. Possible actions that lead to this state are described in the "**MAP data is incorrect**" sub-tree (next section).

"Hacker compromised TMS" attack subtree

Hacker (adversary) compromises TMS server. Possible actions that lead to this state are *both of the following*:

1. Phishing email is sent to IOO employee by hacker.

2. Employee clicks on link from email that downloads malware on the IOO internal network.

Another possible type of action is:

3. Compromise server via means other than email phishing.

"Malware loaded on <component>" attack subtree

Both the RSU and the TSC attack sub-trees are described here since they are very similar. Malware here is an extraneous piece of software that causes incorrect SPaT data or messages to be constructed by the component of the CI system (RSU, TSC infrastructure). Possible actions that lead to this state are any of the following:

1. Software update for the <component> has vulnerability that's being exploited by the malware. Alternatively, the software update itself contains the malware - which can be due to supply chain compromise, e.g., malicious party at the OEM or its suppliers purposely inserts this code. The software update can be from the OEM or from some other third-party supplier.

2. Adversary (hacker) compromises the Traffic Management System (TMS). Then the hacker can use the TMS to load malware onto the <component> via regular management signaling. Possible actions that lead to this state are described in the "Hacker compromised TMS" attack sub-tree.

3. Hacker connects their laptop to the <component> and uses this connection to load malware directly. A possible action that leads to this state is the following:

    3.1 Hacker has managed to open the cabinet door. This may be either because either of the following actions (not shown in diagram for simplicity):

        3.1.1 Hacker fraudulently obtained a key to the cabinet.

        3.1.2 Hacker forced open the cabinet door.

Mitigations

Mitigations for the events/adversary activity listed above are listed in Table .

Table C1 - Mitigations - RSU outputs incorrect SPaT messages

Adversary Action Name	Possible Mitigation(s)
1.1 RSU signs with invalid certificate	1. Track RSU certificate validity time and automatically renew it before it expires. 2. Ensure correct PSID appears in RSU certificates.
1.2 Malware loaded on RSU	1. Employ Software checking at RSU. 2. Scan RSU software with up-to-date tools to detect vulnerabilities or malware. 3. Employ secure boot on RSU. 4. See child attacks mitigations.
1.2.1 Hacker compromised the TMS	1. Employ Software checking at RSU. 2. Scan RSU software with up-to-date tools to detect vulnerabilities or malware. 3. Employ secure boot on RSU. **4. See entry 1.4.1.2.**
1.2.2 Software update has vulnerability or malware	1. Employ Software checking at RSU. 2. Scan RSU software with up-to-date tools to detect vulnerabilities or malware. 3. Employ secure boot on RSU. 4. Disallow remote software or firmware updates. 5. Ensure security of channel to receive updates from the OEM (e.g., OEM's signature on binary executable).
1.2.3 Hacker connected laptop to RSU	1. Mount RSU very high up on pole. 2. See child attacks mitigations.
1.2.3.1 Hacker opened cabinet	1. Mount RSU very high up on pole. 2. Monitor alerts at the TMS of open cabinet where RSU hardware is located. 3. (Possible recovery): Have means to immediately isolate (from network) the TSC if the opening was unauthorized. 4. (Possible detection): Use tamper-evident sealing.
1.3 RSU is misconfigured	1. Ensure time at the RSU matches true system time (Periodic check). 2. Ensure MAP data correctness to the RSU. 3. Periodically check configuration settings at the RSU (from the TMS).
1.4 TSC infrastructure sends incorrect data	1. Ensure RSU software employs input validation. 2. See child attacks mitigations.
1.4.1 TSC data is corrupted	1. Ensure RSU software employs input validation. 2. See child attacks mitigations.
1.4.1.1 TSC data is tampered/spoofed in transit from RSU	1. Ensure RSU software employs input validation. 2. Connection is physically difficult to access. 3. Connection uses cryptographic authentication.
1.4.1.2. Hacker compromised the TMS	*(see Note below)* 1. Employ state-of-the-art Intrusion Prevention/Detection Systems (IPS/IDS) into the TMS network. 2. Employ threat-informed defenses and keep the set of threats up to date. 3. Employ firewalls with clearly set policies to reduce access to the TMS for external networks. 4. Ensure TMS is not accessible from the public Internet.
1.4.1.2.1 Phishing email to IOO employee	1. *1 - 4 above (1.4.1.2)*. 5. Use email filtering tools.
1.4.1.2.2 Employee clicks on link from phishing email	1. *1 - 4 above (1.4.1.2)*. 5. Train IOO employees about email security. 6. Periodically send test emails to determine effectiveness of training.
1.4.1.2.3 Compromise server via means other than email phishing	See mitigation on parent (1.4.1.2).
1.4.2 Malware loaded on the TSC infrastructure component	See entry 1.2 "Malware loaded on the RSU," apply to TSC infrastructure component.
1.5 MAP data is incorrect	See entry 2.4 in "MAP data is incorrect" attack sub-tree (next section).

NOTE: Entry 1.4.1.2: This is a subtree that should be stand-alone since it's referenced elsewhere, so it does not have its parent's mitigations in it explicitly. For a complete mitigation of attack 1.4.1.2, include also mitigations of 1.4.1.

C.3.4 Constructing an Attack Tree: RSU Outputs Incorrect MAP Messages

An example attack tree showing some of the attacks that may cause an RSU to output incorrect MAP messages is shown in Figure below and is provided for illustrative purposes only. Such figures are optional to the IOO documentation. The attack tree can be described in list format, an example of which is shown next.

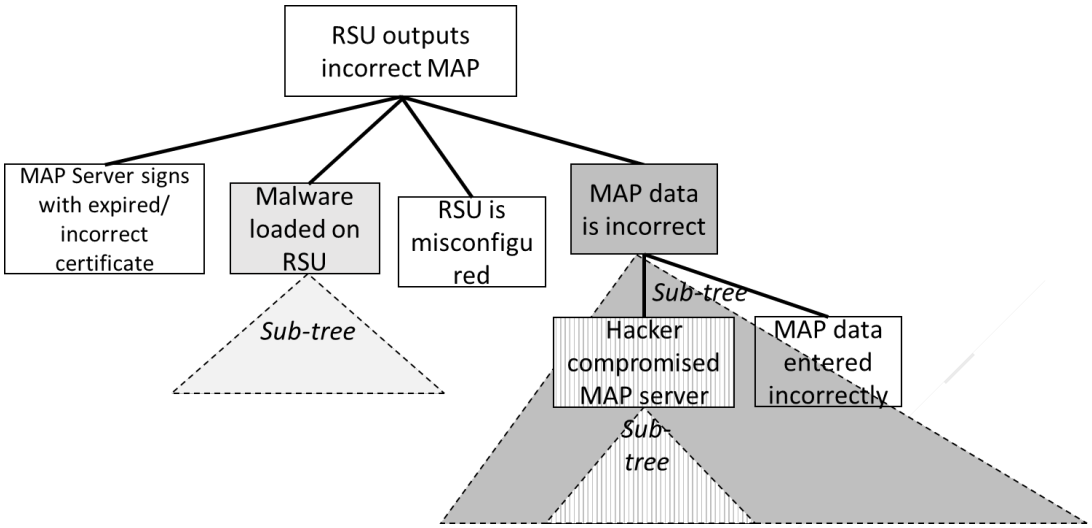

Figure C7 - Attack tree example - RSU outputs incorrect MAP messages

"RSU outputs incorrect MAP messages" attack tree

2. RSU outputs incorrect MAP messages.

Possible actions that lead to this state are any of the following:

2.1 MAP server signs with invalid certificate. Possible actions that lead to this state are any of (not shown in the diagram):

2.1.1 MAP server signs with expired certificate. This may occur because the MAP server's own certificate has expired or one in its chain is expired, and the MAP signing software does not check that the certificate is unexpired before signing.

2.1.2 MAP server signs with certificate with incorrect Provider Service Identifier (PSID). This may occur because the MAP server's certificate has the incorrect PSID, and the MAP signing software does not check that the certificate has the correct permissions before signing.

2.1.3 (Other attacks can be inserted here based on the ways in which a message can be inconsistent with the certificate as specified in IEEE Std 1609.2 - for example, inconsistent SSP, inconsistent geographic region, etc.)

2.2 Malware loaded on RSU causes incorrect MAP messages to be constructed by the RSU. Possible actions that lead to this state are described in the "**Malware loaded on RSU**" sub-tree.

2.3 RSU is misconfigured. See corresponding action (1.3) in the "RSU outputs incorrect SPaT messages" attack tree.

2.4 MAP data is incorrect. Possible actions that lead to this state are described in the "**MAP data is incorrect**" attack sub-tree.

"MAP data is incorrect' attack subtree

Possible actions that lead to this state are any of the following:

2.4.1 MAP data is tampered in transit from TMS to RSU. Possible actions that lead to this state are: Hacker compromised a middlebox (router, switch) in ITS network and is able to alter the data without detection due to lack of transport-layer security (TLS).

2.4.2 Hacker compromised MAP server. Then hacker can use the MAP server to spoof MAP data that is sent. Possible actions that lead to this state are described in the "**Hacker compromised TMS**" attack sub-tree, where the "MAP Server" is substituted for the TMS.

2.4.3 MAP data is entered incorrectly. Possible actions that lead to this state are any of the following (not shown in the diagram):

2.4.3.1 The staff who enters this data or supervises the automatic data upload accidentally enters incorrect data.

2.4.3.2 Staff fails to check for correctness of input data.

2.4.3.3 The data entered is not current.

Mitigations

Mitigations for the events/adversary activity listed above are listed in Table .

Table C2 - Mitigation - RSU outputs incorrect MAP messages

Adversary Action Name	Possible Mitigation(s)
2.1 MAP server signs with invalid certificate	1. Track MAP server certificate validity time and automatically renew it before it expires. 2. Ensure correct PSID appears in MAP server certificate. 3. Ensure RSU checks MAP signature and does not output a MAP if it doesn't pass this check.
2.2 Malware loaded on RSU	1. **See corresponding entry 1.2** in the "RSU outputs incorrect SPaT" mitigations.
2.3 RSU is misconfigured	1. **See corresponding entry 1.3** in the "RSU outputs incorrect SPaT" mitigations.
2.4 MAP data is incorrect	1. Ensure RSU software performs input validation for MAP data. 2. See child attacks mitigations.
2.4.1 MAP data is tampered in transit from TMS to RSU	1. Ensure RSU software performs input validation for MAP data. 2. Employ TLS with integrity protection between TMS and RSU.
2.4.2 Hacker compromised MAP server	1. Ensure RSU performs input validation for MAP data. 2. **See corresponding entry 1.4.1.2** in the "RSU outputs incorrect SPaT" mitigations, with TMS being replaced by MAP server.
2.4.3 MAP data entered incorrectly	1. Attack risk is low, no mitigation.

C.3.5 Constructing an Attack Tree: "RSU outputs incorrect RTCMcorrections messages."

An example attack tree showing some of the ways that may cause an RSU to output incorrect RTCMcorrections messages is similar to that of Figure . The difference with the MAP messages is that RTCM data can be obtained by the RSU from an online source (like a NTRIP provider), GPS receiver or cellular base station nearby, or from the TMS (for example, the TMS does its own calculation). The RSU can sign these messages, or they may be already signed by the source.

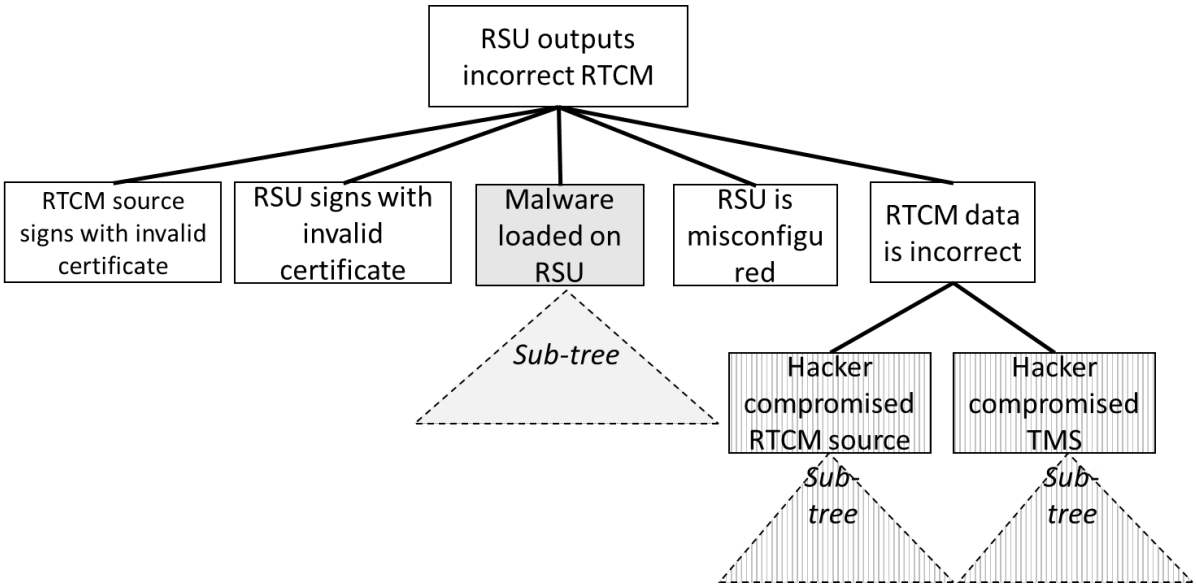

Figure C8 - Attack tree example - RSU outputs incorrect RTCM messages

"RSU outputs incorrect RTCM messages" attack tree

3. RSU outputs incorrect RTCM messages.

Possible actions that lead to this state are any of the following:

3.1 RTCM source signs with invalid certificate.

3.2 RSU signs with invalid certificate. See the corresponding entry (1.1) in the "**RSU outputs incorrect SPaT messages**" attack tree.

3.3 Malware loaded on RSU causes incorrect RTCM messages to be constructed by the RSU. Possible actions that lead to this state are described in the "**Malware loaded on RSU.**"

3.4 RSU is misconfigured. See corresponding entry in the "**RSU outputs incorrect SPaT messages**" attack tree.

3.5 RTCM data is incorrect. Possible actions that lead to this state are any of the following:

3.5.1 Hacker compromised RTCM source. Possible actions that lead to this state are described in the "**Hacker compromised TMS**" attack sub-tree, where the "RTCM Server" is substituted for the TMS. Another possible way is that the cellular base station or RTCM GPS receiver has been compromised.

3.5.2 Hacker compromised TMS. This is for the case when the RTCMs are sourced by the TMS. Possible actions that lead to this state are described in the "**Hacker compromised TMS**" attack sub-tree.

Mitigations

Mitigations for the events/adversary activity listed above are listed in Table .

Table C3 - Mitigation - RSU outputs incorrect RTCM messages

Adversary Action Name	Possible Mitigation(s)
3.1 RTCM source signs with invalid certificate	1. RSU checks RTCM signature and does not output a RTCM if it doesn't pass this check.
3.2 RSU signs with invalid certificate	1. **See corresponding entry 1.1** in the "RSU outputs incorrect SPaT" mitigations
3.3 Malware loaded on RSU	1. **See corresponding entry 1.2** in the "RSU outputs incorrect SPaT" mitigations
3.4 RSU is misconfigured	1. **See corresponding entry 1.3** in the "RSU outputs incorrect SPaT" mitigations
3.5 RTCM data is incorrect	1. Ensure RSU software employs input validation **2. See child attacks for mitigations**
3.5.1 Hacker compromised RTCM server	1. Ensure RSU software employs input validation 2. **See corresponding entry 1.4.1.2** in the "RSU outputs incorrect SPaT" mitigations, with TMS being replaced by RTCM server
3.5.2 Hacker compromised TMS	1. Ensure RSU software employs input validation 2. **See corresponding entry 1.4.1.2** in the "RSU outputs incorrect SPaT" mitigations

C.4 SECURITY REQUIREMENTS TRACEABILITY

This section provides additional information related to security requirements, including the process used to derive and validate the security requirements.

C.4.1 Tracing Functional Requirements to Security Requirements

Derivation of the security requirements used a systematic approach. The Security Task Force looked at each security user need (refer to CTI 4501, 5.4.4) and derived security requirements as appropriate. The traces from the security user needs to security requirements are found in CTI 4501, Table 5, Needs to Requirements Traceability Matrix.

As part of their approach, the CTI Security Task Force also reviewed each functional requirement defined in Section 0 (except 6.3.4, which contains the security requirements) for potential security requirements - i.e., considered if there are any security requirements that should be associated with that functional requirement.

Since the NRTM in CTI 4501, Table 5 traces only user needs to requirements, Table shows the traces from all the functional requirements in CTI 4501 (except security requirements) to the security requirements (if any) that should be considered if the functional requirement is selected. Note that this section, and thus the traces, are informative. CTI 4501, Table 5 is normative.

Table C4 - Functional requirements to security requirements

FR ID	Functional Requirement	SR ID	Security Requirement
CTI 4501: 6.3.1.1.1.1	ProSe Per Packet Priority - SPaT Message	6.3.4.1.51	Protect V2X Radio Parameters
CTI 4501: 6.3.1.1.1.2	ProSe Per Packet Priority - MAP Message	6.3.4.1.51	Protect V2X Radio Parameters
CTI 4501: 6.3.1.1.1.3	ProSe Per Packet Priority - RTCMcorrections Message	6.3.4.1.51	Protect V2X Radio Parameters
CTI 4501/1: 6.3.2.1.1.1	NTCIP 1202 SPaT Information	6.3.4.3*	Trustworthiness of TSC-Originating Information *
CTI 4501/1: 6.3.2.1.1.2	TSCBM SPaT Information	6.3.4.3*	Trustworthiness of TSC-Originating Information *
CTI 4501/1: 6.3.2.1.1.3	SPaT Message - Immediate Forward	6.3.4.3*	Trustworthiness of TSC-Originating Information *
CTI 4501/1: 6.3.2.1.2	TSC Signal State Periodicity	6.3.4.3*	Trustworthiness of TSC-Originating Information *
CTI 4501/1: 6.3.2.1.3	TSC Signal Indication Phase State and SPaT Information Consistency	6.3.4.3*	Trustworthiness of TSC-Originating Information *
CTI 4501/1: 6.3.2.2.1	TSC Infrastructure Manual Control Indication	6.3.4.3*	Trustworthiness of TSC-Originating Information *
CTI 4501/1: 6.3.2.2.2	TSC Infrastructure Stop Time Indication	6.3.4.3*	Trustworthiness of TSC-Originating Information *
CTI 4501/1: 6.3.2.2.3	TSC Infrastructure Cabinet Flash (Exception Flash) Indication	6.3.4.3*	Trustworthiness of TSC-Originating Information *
CTI 4501/1: 6.3.2.2.4	TSC Infrastructure Controller Flash (Operational Flash) Indication	6.3.4.3*	Trustworthiness of TSC-Originating Information *
CTI 4501/1: 6.3.2.2.5	TSC Infrastructure Preemption Operation Indication	6.3.4.3*	Trustworthiness of TSC-Originating Information *
CTI 4501/1: 6.3.2.2.6	TSC Infrastructure Priority Operation Indication	6.3.4.3*	Trustworthiness of TSC-Originating Information *
CTI 4501/1: 6.3.2.2.7	TSC Infrastructure Fixed Time Control Indication	6.3.4.3*	Trustworthiness of TSC-Originating Information *
CTI 4501/1: 6.3.2.2.8	TSC Infrastructure Non-Fixed Time Control	6.3.4.3.1	TSC Infrastructure Protection: Invalid Signal Timing Information
CTI 4501/1: 6.3.2.3.1	TSC Infrastructure Assured Green End Time (AGET)	None	
CTI 4501/1: 6.3.2.3.2.1	Support Green Extension for AGP	6.3.4.5.1	Protection from Unnecessary AGP
CTI 4501/1: 6.3.2.4.1	Receive BSM Messages	6.3.4.4.1	Validate Security of Approaching Vehicle V2X Messages
		6.3.4.4.2	Validate Approaching Vehicle V2X Messages: Replay
		6.3.4.4.3	Validate Approaching Vehicle V2X Messages: Misbehavior Detection
		6.3.4.4.4	Validate Approaching Vehicle V2X Messages: Misbehavior Reporting
		6.3.4.4.5	Validate Approaching Vehicle V2X Messages: Distinguish Between Senders
CTI 4501/1: 6.3.2.4.2	BSM Messages Filtered by Detection Zones	6.3.4.4.6	Security for Use of RSU BSM Filtering for RDZ
CTI 4501/1: 6.3.2.4.3	BSM Message Rate for AGP and RLVW		

FR ID	Functional Requirement	SR ID	Security Requirement
		6.3.4.4.7	Security for Configuration of RSU BSM Filtering for RDZ
CTI 4501/1: 6.3.3.1.1.1	SPaT Message - SAE J2735	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.1.1.2	SPaT Message - Mandatory Data Elements	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.1.1.3	SPaT Message - Required Data Elements	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.1.1.4	SPaT Message PSID	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/2: 6.3.3.1.1.5	MAP Message - SAE J2735	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
CTI 4501/2: 6.3.3.1.1.6	MAP Message - Mandatory Data Elements	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.1.1.7	MAP Message - Required Data Elements	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.1.1.8	MAP Message PSID	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
SAE J3258: 6.1.1	RTCMcorrections Message - SAE J2735	6.3.4.9.1	List of CI Data Entities that Affect RTCM Contents
		6.3.4.9.2	Prevent Invalid RTCM Contents or Behavior
SAE J3258: 6.1.2	RTCMcorrections Message - Mandatory Data Elements	6.3.4.9.1	List of CI Data Entities that Affect RTCM Contents
		6.3.4.9.2	Prevent Invalid RTCM Contents or Behavior
		6.3.4.9.3	External RTCM Message Generation or Partial Generation: Data Source
SAE J3258: 6.1.3	RTCMcorrections Message - Required Data Elements	6.3.4.9.1	List of CI Data Entities that Affect RTCM Contents
		6.3.4.9.2	Prevent Invalid RTCM Contents or Behavior

FR ID	Functional Requirement	SR ID	Security Requirement
		6.3.4.9.3	External RTCM Message Generation or Partial Generation: Data Source
SAE J3258: 6.1.4	RTCMcorrections Message PSID	6.3.4.9.1	List of CI Data Entities that Affect RTCM Contents
		6.3.4.9.2	Prevent Invalid RTCM Contents or Behavior
		6.3.4.9.3	External RTCM Message Generation or Partial Generation: Data Source
CTI 4501/1: 6.3.3.1.2.1	Broadcast SPaT Message	6.3.4.3.1	TSC Infrastructure Protection: Invalid Signal Timing Information
		6.3.4.3.2	TSC Infrastructure Protection: Invalid Format for Signal Timing Information
		6.3.4.3.3	TSC Infrastructure Protection: Incorrect Format for Signal Timing Information
CTI 4501: 6.3.3.1.3.1	Transport Message Size - WAVE	6.3.4.2.22	Security Size Overhead
CTI 4501/2: 6.3.3.1.3.2.1	Nodes by Offsets	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.1.3.2.2.1	Computed Lane - Lane Identifier	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.1.3.2.2.2	Computed Lane - X-Offset	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.1.3.2.2.3	Computed Lane - Y-Offset	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.1.3.2.2.4	Computed Lane - Angle	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501: 6.3.3.1.4.1	Data Coverage - Every Ingress Lane	6.3.4.17.1	Prevent Change in Data Coverage

FR ID	Functional Requirement	SR ID	Security Requirement
		6.3.4.17.2	Detect Change in Data Coverage
CTI 4501: 6.3.3.1.4.2	Advanced Notification - Time	6.3.4.17.3	Prevent Change in Radio Power
		6.3.4.17.4	Detect Change in Radio Power
CTI 4501/2: 6.3.3.1.5.2	MAP Message - Broadcast Periodicity	6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
CTI 4501/1: 6.3.3.1.5.1	SPaT Message - Broadcast Latency and Accuracy - Commanded	6.3.4.3.1	Prevent Invalid SPaT Contents or Behavior
		6.3.4.3.2	TSC Infrastructure Protection: Invalid Signal Timing Information
		6.3.4.3.3	TSC Infrastructure Protection: Invalid Format for Signal Timing Information
		6.3.4.3.4	TSC Infrastructure Protection: Invalid Contents for Signal Timing Data
		6.3.4.3.5	Information About Availability of SPaT Information
CTI 4501/1: 6.3.3.1.6.1	Completeness - SPaT Message	6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/2: 6.3.3.1.6.2	Completeness - MAP Message	6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
CTI 4501/1: 6.3.3.1.6.3	SPaT Message - Time Mark Accuracy	6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
6.3.3.2.1	Time Accuracy	6.3.4.6*	Time Source Trustworthiness *
CTI 4501/1: 6.3.3.2.2.1	SPaT Message - Revision Counter Increment	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.2.2.2	SPaT Message - Revision Counter Not Increment	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/2: 6.3.3.2.2.3	MAP Message - Revision Counter Increment	6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
CTI 4501/2: 6.3.3.2.2.4	MAP Message - Revision Counter Not Increment	6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
CTI 4501/2: 6.3.3.2.2.5	MAP Message - Intersection Revision Counter Increment	6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
CTI 4501/2: 6.3.3.2.2.6	MAP Message - Intersection Revision Counter Not Increment	6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
J3258: 6.2.1	RTCMcorrections Message - Sequence Number Increment	6.3.4.9.2	Prevent Invalid RTCM Contents or Behavior
J3258: 6.2.2	RTCMcorrections Message - Sequence Number Not Increment	6.3.4.9.2	Prevent Invalid RTCM Contents or Behavior
CTI 4501/1: 6.3.3.2.3.1	SPaT Message - Message Time Stamp	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.2.3.2	SPaT Message - Intersection Time Stamp	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.1	Intersection Identification Requirements	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents

FR ID	Functional Requirement	SR ID	Security Requirement
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.1.1	Intersection Signal Timing Information	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.1.2	Intersection Identifier	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.1.3	Road Authority Identifier	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.2.1	Manual Control	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.2.2	Stop Time	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.2.3	Failure Flash	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.2.4	Preemption	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.2.5	Priority	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.2.6	Fixed Time	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.2.7	Traffic Dependent Mode	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.2.8	Standby Mode	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.2.9	Failure Mode	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.2.10	Controller Off	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.2.11	Recent MAP Update	6.3.4.8.2	Prevent Invalid MAP Contents or Behavior

FR ID	Functional Requirement	SR ID	Security Requirement
		6.3.4.8.4	Prevent Inconsistency of MAP and Road Geometry or Use: False Positives
		6.3.4.8.6	Detect Inconsistency of MAP and Road Geometry or Use
		6.3.4.8.7	Manage Inconsistency of MAP and Road Geometry or Use
		6.3.4.10.1	SPaT and MAP Version Consistency
CTI 4501/1: 6.3.3.3.2.12	New Lane IDs	6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.4	Prevent Inconsistency of MAP and Road Geometry or Use: False Positives
		6.3.4.8.6	Detect Inconsistency of MAP and Road Geometry or Use
		6.3.4.8.7	Manage Inconsistency of MAP and Road Geometry or Use
CTI 4501/1: 6.3.3.3.2.13	No MAP Available	6.3.4.11.3	Correctness of MAP Availability Indications
		6.3.4.11.4	Correctness of MAP Unavailability Indications
CTI 4501/1: 6.3.3.3.2.14	No SPaT Available	6.3.4.11.1	Correctness of SPaT Availability Indications
		6.3.4.11.2	Correctness of SPaT Unavailability Indications
CTI 4501/1: 6.3.3.3.3.1	Current Movement State for a Signal Group	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.3.2	Unknown Current Movement State for a Signal Group	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.3.3	Flashing Yellow Arrow Permissive Movement	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.3.4	Protected and Permissive Clearance	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.3.5	Resolve Protected Versus Permissive Movement	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.3.6	Yield Causes Permissive	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.3.7	Right-of-Way Causes Protected	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.3.8	WALK State Enumeration	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents

FR ID	Functional Requirement	SR ID	Security Requirement
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.3.9	Flashing DON'T WALK State Enumeration	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.3.10	Steady DON'T WALK State Enumeration	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.3.11	Movement State for Signal Groups Identified	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.3.12	Dark Pedestrian Indications	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.3.13	Prohibited Movements	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.3.14	Movements Allowed After a Stop	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.4.1	Next Movement State	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.4.2	Unknown Next Movement State	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.4.3	No Past State	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.5.1	Time Change Details	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.5.2	Unknown Time Change Detail	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.5.3	Minimum End Time	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.5.4	Maximum End Time	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.5.5	Unknown Maximum End Time	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents

FR ID	Functional Requirement	SR ID	Security Requirement
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.5.6	Current Movement State Start Time Unknown	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.5.7	Next Movement State Start Time	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.5.8	Next State Start Time Equals Current State Minimum End Time	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.6.1	Time of Next Allowed Movement	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.7	Enabled Lanes Indication	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/1: 6.3.3.3.8	SPaT Message - Accuracy	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/2: 6.3.3.4.1.1	Intersection Geometry Information	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.2	Intersection Geometry - Road Authority Identifier	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.3	Intersection Geometry - Intersection Identifier	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.4.1	Intersection Reference Point - Position	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.4.2	Intersection Reference Point - Description	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior

FR ID	Functional Requirement	SR ID	Security Requirement
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.5	Default Lane Width	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.6	Lane Identifier	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.7	Center of Vehicle Lane Geometry	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.8	Center of Crosswalk Lane Geometry	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.9	Center of Pedestrian Landings Geometry	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.10	Lane Description	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.11	First Node Point - Ingress Vehicle Lane	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.12	First Node Point - Egress Vehicle Lane	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior

FR ID	Functional Requirement	SR ID	Security Requirement
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.13	Node Offset from Intersection Reference Point	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.14	Node Elevation Offset from Intersection Reference Point	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.15	Offset from Previous Node	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.16	Elevation Offset from Previous Node	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.17	Advanced Notification - Ingress Vehicle Lane	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.18	End Nodes - Crosswalk Lane	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.19	End Nodes - Pedestrian Landing	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.20	Maximum Distance between Nodes	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior

FR ID	Functional Requirement	SR ID	Security Requirement
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.21	Maximum Number of Nodes	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.22	Node Lane Width	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.1.23	Node Lane Width Change	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.2.1	Direction of Travel	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.2.2	Lane Sharing	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.2.3	Lane Type Attributes	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.2.4	Lane Attributes - Vehicle	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.2.5	Lane Attributes - Crosswalk	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior

FR ID	Functional Requirement	SR ID	Security Requirement
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.2.6	Lane Attributes - Bicycle	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.2.7	Lane Attributes - Tracked Vehicles	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.2.8	Lane Attributes - Parking	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.3	Lane Maneuvers	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.4.1	Lane Connections	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.4.2	Connection Egress Lane	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/2: 6.3.3.4.4.3	Connection Maneuvers	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/2: 6.3.3.4.4.4	Connection Signal Group	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/2: 6.3.3.4.4.5	Include Only Permitted Connections	6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents
		6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior
CTI 4501/2: 6.3.3.4.5.1	Default Speed Limit	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior

FR ID	Functional Requirement	SR ID	Security Requirement
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.5.2	Change in Lane Speed Limit	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.6	Revocable Lanes	6.3.4.8.1	List of CI Data Entities that Affect MAP Contents
		6.3.4.8.2	Prevent Invalid MAP Contents or Behavior
		6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source
CTI 4501/2: 6.3.3.4.7.1	Matching SPaT and MAP Version	6.3.4.10.1	SPaT and MAP Version Consistency
CTI 4501/2: 6.3.3.4.7.2	Matching Intersection Reference Identifiers	6.3.4.10.2	SPaT and MAP Intersection Identifier Consistency
CTI 4501/2: 6.3.3.4.7.3	Complete List of Signal Group Identifiers	6.3.4.10.1	SPaT and MAP Version Consistency
CTI 4501/2: 6.3.3.4.7.4	Matching Signal Group Identifier Movements	6.3.4.10.1	SPaT and MAP Version Consistency
SAE J3258: 6.3.1	Positioning Corrections	6.3.4.9*	RTCM Message Contents Trustworthiness *
CTI 4501: 6.3.5.1.1	Mean-Time-Between-Failures (MTBF)	None	
CTI 4501: 6.3.5.1.2	Operational Uptime	None	
CTI 4501: 6.3.5.2.1	Documented Plan for Life Cycle Operations & Maintenance	6.3.4.13.15	Maintenance Security Needs
		6.3.4.13.2	List of Operator-Notifiable Events
		6.3.4.13.3	List of Systemic Failure Events
		6.3.4.13.4	Cyberattack Must be Addressed
		6.3.4.13.5	Recovery Plan from Systemic Failure
		6.3.4.13.6	Recovery from Systemic Failure Only When Necessary
		6.3.4.13.7	Preserve Access Control During Systemic Failure
		6.3.4.13.8	Robustness of Recovery from Systemic Failure
		6.3.4.13.9	Assurance of Recovery from Systemic Failure
		6.3.4.13.10	Source Assurance for Recovery from Failure for Internal Data Sources or Processors
		6.3.4.13.11	Automated Recovery from Failure for the CI is not to be an Attack Vector
		6.3.4.13.12	Vulnerability Management for Potential
		6.3.4.13.13	Security Validation
CTI 4501: 6.3.5.3.1	Support Normal Mode	6.3.4.16.1	Correct Operational Mode Protection

FR ID	Functional Requirement	SR ID	Security Requirement
		6.3.4.16.3	Protection Against Improper Operation in Maintenance Mode
		6.3.4.16.4	Protecting Determinations that Normal Mode Transition Criteria are Met
CTI 4501: 6.3.5.3.2	Maintenance Mode	6.3.4.16.1	Correct Operational Mode Protection
		6.3.4.16.3	Protection Against Improper Operation in Maintenance Mode
		6.3.4.16.4	Protecting Determinations that Normal Mode Transition Criteria are Met
CTI 4501: 6.3.5.3.3	Report Operational Mode Status	6.3.4.16.2	Correct Mode and Status Reporting
CTI 4501: 6.3.5.3.4	Support Maintenance Mode Fallback	6.3.4.16.1	Correct Operational Mode Protection
		6.3.4.16.3	Protection Against Improper Operation in Maintenance Mode
		6.3.4.16.4	Protecting Determinations that Normal Mode Transition Criteria are Met
CTI 4501: 6.3.5.3.5	Perform Validation	6.3.4.13.13	Security Validation
CTI 4501: 6.3.5.3.6	Command Maintenance Mode	6.3.4.16.1	Correct Operational Mode Protection
		6.3.4.16.3	Protection Against Improper Operation in Maintenance Mode
		6.3.4.16.4	Protecting Determinations that Normal Mode Transition Criteria are Met
		6.3.4.16.5	Correct Representation of Operating Mode
CTI 4501: 6.3.5.3.7	Automatic Return to Normal Mode	6.3.4.16.1	Correct Operational Mode Protection
		6.3.4.16.3	Protection Against Improper Operation in Maintenance Mode
		6.3.4.16.4	Protecting Determinations that Normal Mode Transition Criteria are Met
		6.3.4.16.5	Correct Representation of Operating Mode
CTI 4501: 6.3.5.4.1	System Malfunction Alert	6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors
		6.3.4.1.24	Events to be Monitored by Self-Monitoring
		6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring
		6.3.4.1.26	Self-Monitoring for Internal CI Data Entities: Robustness
		6.3.4.1.27	Self-Monitoring for Internal CI Data Entities: Error Management
		6.3.4.1.32	Self-Monitoring for Internal CI Data Entities: Logging
		6.3.4.1.33	Log Generation for External CI Data Entities
		6.3.4.1.34	Log Events for CI Data Entities

FR ID	Functional Requirement	SR ID	Security Requirement
		6.3.4.1.35	Changes in Logged Information
		6.3.4.1.36	Access to Logs for CI Data Entities
		6.3.4.1.37	Timely Access to Logs for CI Data Entities
		6.3.4.14.1	CI Performance Monitoring System
		6.3.4.14.2	Events to be Monitored by
		6.3.4.14.3	CPMS: Other System Monitoring
		6.3.4.14.4	CPMS: Robustness Against Invalid Input
		6.3.4.14.5	CPMS: Error Management
CTI 4501: 6.3.5.4.2	Detect System Exceptions	6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors
		6.3.4.1.24	Events to be Monitored by Self-Monitoring
		6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring
		6.3.4.1.26	Self-Monitoring for Internal CI Data Entities: Robustness
		6.3.4.1.27	Self-Monitoring for Internal CI Data Entities: Error Management
		6.3.4.1.32	Self-Monitoring for Internal CI Data Entities: Logging
		6.3.4.1.33	Log Generation for External CI Data Entities
		6.3.4.1.34	Log Events for CI Data Entities
		6.3.4.1.35	Changes in Logged Information
		6.3.4.1.36	Access to Logs for CI Data Entities
		6.3.4.1.37	Timely Access to Logs for CI Data Entities
		6.3.4.14.1	CI Performance Monitoring System
		6.3.4.14.2	Events to be Monitored by
		6.3.4.14.3	CPMS: Other System Monitoring
		6.3.4.14.4	CPMS: Robustness Against Invalid Input
		6.3.4.14.5	CPMS: Error Management
CTI 4501: 6.3.5.4.3	System Exception Reporting	6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors
		6.3.4.1.24	Events to be Monitored by Self-Monitoring
		6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring
		6.3.4.1.26	Self-Monitoring for Internal CI Data Entities: Robustness
		6.3.4.1.27	Self-Monitoring for Internal CI Data Entities: Error Management

FR ID	Functional Requirement	SR ID	Security Requirement
		6.3.4.1.32	Self-Monitoring for Internal CI Data Entities: Logging
		6.3.4.1.33	Log Generation for External CI Data Entities
		6.3.4.1.34	Log Events for CI Data Entities
		6.3.4.1.35	Changes in Logged Information
		6.3.4.1.36	Access to Logs for CI Data Entities
		6.3.4.1.37	Timely Access to Logs for CI Data Entities
		6.3.4.14.1	CI Performance Monitoring System
		6.3.4.14.2	Events to be Monitored by
		6.3.4.14.3	CPMS: Other System Monitoring
		6.3.4.14.4	CPMS: Robustness Against Invalid Input
		6.3.4.14.5	CPMS: Error Management
CTI 4501: 6.3.5.4.4	System Component Diagnostics	6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors
		6.3.4.1.24	Events to be Monitored by Self-Monitoring
		6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring
		6.3.4.1.26	Self-Monitoring for Internal CI Data Entities: Robustness
		6.3.4.1.27	Self-Monitoring for Internal CI Data Entities: Error Management
		6.3.4.1.32	Self-Monitoring for Internal CI Data Entities: Logging
		6.3.4.1.33	Log Generation for External CI Data Entities
		6.3.4.1.34	Log Events for CI Data Entities
		6.3.4.1.35	Changes in Logged Information
		6.3.4.1.36	Access to Logs for CI Data Entities
		6.3.4.1.37	Timely Access to Logs for CI Data Entities
		6.3.4.14.1	CI Performance Monitoring System
		6.3.4.14.2	Events to be Monitored by
		6.3.4.14.3	CPMS: Other System Monitoring
		6.3.4.14.4	CPMS: Robustness Against Invalid Input
		6.3.4.14.5	CPMS: Error Management
CTI 4501: 6.3.5.5.1	Support Monitoring System	6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors
		6.3.4.1.24	Events to be Monitored by Self-Monitoring
		6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring

FR ID	Functional Requirement	SR ID	Security Requirement
		6.3.4.1.26	Self-Monitoring for Internal CI Data Entities: Robustness
		6.3.4.1.27	Self-Monitoring for Internal CI Data Entities: Error Management
		6.3.4.1.32	Self-Monitoring for Internal CI Data Entities: Logging
		6.3.4.1.33	Log Generation for External CI Data Entities
		6.3.4.1.34	Log Events for CI Data Entities
		6.3.4.1.35	Changes in Logged Information
		6.3.4.1.36	Access to Logs for CI Data Entities
		6.3.4.1.37	Timely Access to Logs for CI Data Entities
		6.3.4.14.1	CI Performance Monitoring System
		6.3.4.14.2	Events to be Monitored by
		6.3.4.14.3	CPMS: Other System Monitoring
		6.3.4.14.4	CPMS: Robustness Against Invalid Input
		6.3.4.14.5	CPMS: Error Management
CTI 4501: 6.3.5.5.2	Support Maintenance Mode in Monitoring	6.3.4.16.1	Correct Operational Mode Protection
		6.3.4.16.3	Protection Against Improper Operation in Maintenance Mode
		6.3.4.16.4	Protecting Determinations that Normal Mode Transition Criteria are Met
CTI 4501: 6.3.5.6.1	Support Software Updates	6.3.4.1.24	Events to be Monitored by Self-Monitoring
		6.3.4.1.26	Self-Monitoring for Internal CI Data Entities: Robustness
		6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware
		6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates
		6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update
		6.3.4.1.49	CI Data Entity Update: Validation
		6.3.4.15.1	Prevent Unauthorized CI Software and Configuration Changes
		6.3.4.15.2	Authenticate and Verify Integrity of All Software/Firmware Updates
		6.3.4.15.3	CI Data Entity Update: Validation
CTI 4501: 6.3.5.7.1	Support Operational Mode Following Recovery	6.3.4.1.28	Recovery from Failure for Internal CI Data Entities

FR ID	Functional Requirement	SR ID	Security Requirement
		6.3.4.1.29	Assurance of Recovery from Failure for Internal CI Data Entities
		6.3.4.1.30	Source Assurance for Recovery from Failure for Internal CI Data Entities
		6.3.4.1.31	Automated Recovery from Failure for Internal CI Data Entities is Not to Be an Attack Vector
		6.3.4.13.8	Robustness of Recovery from Systemic Failure
		6.3.4.13.9	Assurance of Recovery from Systemic Failure
		6.3.4.13.10	Source Assurance for Recovery from Failure for Internal Data Sources or Processors
		6.3.4.13.11	Automated Recovery from Failure for the CI is not to be an Attack Vector
		6.3.4.13.12	Vulnerability Management for Potential
CTI 4501: 6.3.5.7.2	Device Power Interruption Recovery	6.3.4.1.28	Recovery from Failure for Internal CI Data Entities
		6.3.4.1.29	Assurance of Recovery from Failure for Internal CI Data Entities
		6.3.4.1.30	Source Assurance for Recovery from Failure for Internal CI Data Entities
		6.3.4.1.31	Automated Recovery from Failure for Internal CI Data Entities is Not to Be an Attack Vector
		6.3.4.13.8	Robustness of Recovery from Systemic Failure
		6.3.4.13.9	Assurance of Recovery from Systemic Failure
		6.3.4.13.10	Source Assurance for Recovery from Failure for Internal Data Sources or Processors
		6.3.4.13.11	Automated Recovery from Failure for the CI is not to be an Attack Vector
		6.3.4.13.12	Vulnerability Management for Potential
CTI 4501: 6.3.5.7.3	Restore Communications Automatically	6.3.4.1.28	Recovery from Failure for Internal CI Data Entities
		6.3.4.1.29	Assurance of Recovery from Failure for Internal CI Data Entities
		6.3.4.1.30	Source Assurance for Recovery from Failure for Internal CI Data Entities
		6.3.4.1.31	Automated Recovery from Failure for Internal CI Data Entities is Not to Be an Attack Vector

FR ID	Functional Requirement	SR ID	Security Requirement
		6.3.4.13.8	Robustness of Recovery from Systemic Failure
		6.3.4.13.9	Assurance of Recovery from Systemic Failure
		6.3.4.13.10	Source Assurance for Recovery from Failure for Internal Data Sources or Processors
		6.3.4.13.11	Automated Recovery from Failure for the CI is not to be an Attack Vector
		6.3.4.13.12	Vulnerability Management for Potential
CTI 4501: 6.3.5.7.4	Process Recovery	6.3.4.1.28	Recovery from Failure for Internal CI Data Entities
		6.3.4.1.29	Assurance of Recovery from Failure for Internal CI Data Entities
		6.3.4.1.30	Source Assurance for Recovery from Failure for Internal CI Data Entities
		6.3.4.1.31	Automated Recovery from Failure for Internal CI Data Entities is Not to Be an Attack Vector
		6.3.4.13.8	Robustness of Recovery from Systemic Failure
		6.3.4.13.9	Assurance of Recovery from Systemic Failure
		6.3.4.13.10	Source Assurance for Recovery from Failure for Internal Data Sources or Processors
		6.3.4.13.11	Automated Recovery from Failure for the CI is not to be an Attack Vector
		6.3.4.13.12	Vulnerability Management for Potential

C.4.2 Tracing Security Requirements to User Needs and Functional Requirements

In addition to the top-down (user needs to requirements) approach mentioned in C.4.1 during the derivation of the security requirements, the Security TF also performed a bottom-up analysis (requirements to user needs) of the security requirements to check for completeness, consistency, and correctness (of the security requirements).

Table lists each security requirement in CTI 4501 then shows each user need and functional requirements that the security requirement traces to. Table is for informational purposes only and allows a user to view what user needs or other functional requirements traces that security requirement has.

Table C5 - Traceability - security requirements to user needs and functional requirements

Security ID	Security Requirement	CTI 4501 ID	User Need or Functional Requirement
6.3.4	Security Requirements		
6.3.4.1	Data Trustworthiness: Sources and Processing		
6.3.4.1.1	Internal Data Sources and Processing	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.2	Manual Data	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.3*	Data Trustworthiness: Specific *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.3	Internal Manual Data Sources	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.3*	Data Trustworthiness: Specific *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.4	Permitted Data from Manual Data Sources	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.3*	Data Trustworthiness: Specific *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.5	External CI Data Entities	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.6	Authorized CI Data Entities	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.7	Authenticated CI Data Entities	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.8	Integrity of Operations for Internal CI Data Entities	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.9	Integrity of Operational Mode for Internal CI Data Entities	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.10	Integrity of Operational Mode Indications for Internal CI Data Entities	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.11	Physical Access to Internal CI Data Entities	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.12	Physical Access to Internal CI Data Entities During Outages or Degraded Operations	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.13	Logical Access to Internal CI Data Entities	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.14	Logical Access to Internal CI Data Entities During Outages or Degraded Operations	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.15	Mitigate Malicious Access to Internal CI Data Entities	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.3.1	Data Sources: Resilience

Security ID	Security Requirement	CTI 4501 ID	User Need or Functional Requirement
		5.4.4.3.3	Data Processing: Resilience
6.3.4.1.16	Access Control on Internal CI Data Entities During Life Cycle	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.5.2*	Life Cycle Security Needs *
6.3.4.1.17	Integrity of Operations for External CI Data Entities	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.18	Mitigate Malicious Access to External Data Sources and Processing	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.3.1	Data Sources: Resilience
		5.4.4.3.3	Data Processing: Resilience
6.3.4.1.19	Access Privileges for Data Sources and Processing	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.20	Access Privileges for Manually Entered Data	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.3*	Data Trustworthiness: Specific *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.21	Record of Accesses to CI Data Entities	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.22	Detect Data Injection from Unauthorized CI Data Entities	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.5.2*	Life Cycle Security Needs *
6.3.4.1.23	Self-Monitoring for Internal CI Data Entities: Detect Significant Errors	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.3.1	Data Sources: Resilience
		5.4.4.3.3	Data Processing: Resilience
		5.4.4.4.3	Confidential Information Within Diagnostics Systems
		5.4.4.4.4	Correct Information Within Diagnostics System
		5.4.4.4.5	Confidential Information Within Performance Monitoring Systems
		5.4.4.4.6	Correct Information Within Performance Monitoring Systems
		5.4.4.5.2*	Life Cycle Security Needs *
		6.3.5.4*	System Diagnostic Interface Requirements*
		6.3.5.5.1	Support Monitoring System
6.3.4.1.24	Events to be Monitored by Self-Monitoring	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.5.2*	Life Cycle Security Needs *
		5.4.4.5.4.2	Upgrade System: Correct Status
		6.3.5.6.1	Support Software Updates
6.3.4.1.25	Self-Monitoring for Internal CI Data Entities: Other System Monitoring	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.4.1	Diagnostics For Security Issues
		5.4.4.5.2*	Life Cycle Security Needs *

Security ID	Security Requirement	CTI 4501 ID	User Need or Functional Requirement
6.3.4.1.26	Self-Monitoring for Internal CI Data Entities: Robustness	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.4.1	Diagnostics For Security Issues
		5.4.4.4.4	Correct Information Within Diagnostics System
		5.4.4.4.6	Correct Information Within Performance Monitoring Systems
		5.4.4.5.2*	Life Cycle Security Needs *
		5.4.4.5.4.2	Upgrade System: Correct Status
6.3.4.1.27	Self-Monitoring for Internal CI Data Entities: Error Management	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.3.1	Data Sources: Resilience
		5.4.4.3.3	Data Processing: Resilience
		5.4.4.5.2*	Life Cycle Security Needs *
6.3.4.1.28	Recovery from Failure for Internal CI Data Entities	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.3.2	Data Sources: Recovery
		5.4.4.3.4	Data Processing: Recovery
		6.3.5.7.1	Support Operational Mode Following Recovery
		6.3.5.7.3	Restore Communications Automatically
		6.3.5.7.4	Process Recovery
6.3.4.1.29	Assurance of Recovery from Failure for Internal CI Data Entities	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.3.2	Data Sources: Recovery
		5.4.4.3.4	Data Processing: Recovery
6.3.4.1.30	Source Assurance for Recovery from Failure for Internal CI Data Entities	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.3.2	Data Sources: Recovery
		5.4.4.3.4	Data Processing: Recovery
6.3.4.1.31	Automated Recovery from Failure for Internal CI Data Entities is Not to Be an Attack Vector	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.3.2	Data Sources: Recovery
		5.4.4.3.4	Data Processing: Recovery
6.3.4.1.32	Self-Monitoring for Internal CI Data Entities: Logging	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.33	Log Generation for External CI Data Entities	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.34	Log Events for CI Data Entities	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.35	Changes in Logged Information	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.36	Access to Logs for CI Data Entities	5.4.4.1*	Data Trustworthiness *

Security ID	Security Requirement	CTI 4501 ID	User Need or Functional Requirement
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
	Timely Access to Logs for CI Data Entities		
6.3.4.1.38	List of Communications Nodes on which Data Could Be Modified	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.39	Communications Nodes on which Data is Manipulable Count as Data Transformation Components	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.40	Availability of CI Data	5.4.4.3.1	Data Sources: Resilience
		5.4.4.3.3	Data Processing: Resilience
6.3.4.1.41	Mitigate Failures of Availability for CI Data	5.4.4.3.1	Data Sources: Resilience
		5.4.4.3.3	Data Processing: Resilience
6.3.4.1.42	Storage Integrity for Internal CI Data Entities: Risk Assessment	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.4.4	Correct Information Within Diagnostics System
		5.4.4.4.6	Correct Information Within Performance Monitoring Systems
6.3.4.1.43	Storage Integrity for CI Data Entities: Risk Mitigation	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.1.44	List of Privacy-Sensitive Information per CI Data Entity	?	
6.3.4.1.45	Protecting Privacy-Sensitive Information per CI Data Entity	?	
6.3.4.1.46	CI Data Entity Update: Authorized Sources of CI Software and Firmware	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.5.4.1	Upgrade System: Correct Operation
6.3.4.1.47	CI Data Entity Update: Authenticate and Verify Integrity of All Software Firmware Updates	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.5.4.1	Upgrade System: Correct Operation
6.3.4.1.48	CI Data Entity Update: Authorized Initiation of Software and Firmware Update	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.5.4.1	Upgrade System: Correct Operation
6.3.4.1.49	CI Data Entity Update: Validation	5.4.4.1*	Data Trustworthiness *
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.5.4.1	Upgrade System: Correct Operation
6.3.4.1.50	CI Data Entity Update: Correct Status	5.4.4.5.4.2	Upgrade System: Correct Status
6.3.4.1.51	Protect V2X Radio Parameters	6.3.1.1*	LTE-V2X Traffic Class Settings
6.3.4.1.52	Threat Analysis	5.4.4.1.3*	Data Trustworthiness: Specific
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.2.2	Secure Communications for CI Data Logical Interfaces	5.4.4.1.3*	Data Trustworthiness: Specific
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI

Security ID	Security Requirement	CTI 4501 ID	User Need or Functional Requirement
6.3.4.2.3	Secure Communications: Integrity	5.4.4.1.3*	Data Trustworthiness: Specific
		5.4.4.2.1	Integrity of Data Passing Across Interfaces Within the CI
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.3.1	Data Sources: Resilience
		5.4.4.3.3	Data Processing: Resilience
6.3.4.2.4	Secure Communications: Integrity of External CI Data Outbound Logical Interfaces	5.4.4.1.3*	Data Trustworthiness: Specific
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.2.3	Integrity of Messages Sent From CI
6.3.4.2.5	Secure Communications: Replay Protection	5.4.4.1.3*	Data Trustworthiness: Specific
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.3.1	Data Sources: Resilience
		5.4.4.3.3	Data Processing: Resilience
6.3.4.2.6	Secure Communications: Plausibility for Received Data	5.4.4.1.3*	Data Trustworthiness: Specific
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.3.1	Data Sources: Resilience
		5.4.4.3.3	Data Processing: Resilience
6.3.4.2.7	Secure Communications: CI-Internal Logical Component Authentication	5.4.4.1.3*	Data Trustworthiness: Specific
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.3.1	Data Sources: Resilience
		5.4.4.3.3	Data Processing: Resilience
6.3.4.2.8	Secure Communications: CI-Internal Physical Component Authentication	5.4.4.1.3*	Data Trustworthiness: Specific
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.3.1	Data Sources: Resilience
		5.4.4.3.3	Data Processing: Resilience
6.3.4.2.9	Secure Communications: Authentication of External CI Data Logical Interfaces	5.4.4.1.3*	Data Trustworthiness: Specific
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.3.1	Data Sources: Resilience
		5.4.4.3.3	Data Processing: Resilience
6.3.4.2.10	Secure Communications: Authentication of External CI Data Outbound Logical Interfaces	5.4.4.1.3*	Data Trustworthiness: Specific
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.2.11	Secure Communications: Check Authentication for Received Data	5.4.4.1.3*	Data Trustworthiness: Specific
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.3.1	Data Sources: Resilience
		5.4.4.3.3	Data Processing: Resilience
6.3.4.2.12	Secure Communications: Manage Received Data for Which Checks Have Failed	5.4.4.1.3*	Data Trustworthiness: Specific
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.3.1	Data Sources: Resilience
		5.4.4.3.3	Data Processing: Resilience
6.3.4.2.13	Secure Communications: External Data Entities for Which Checks Have Failed	5.4.4.1.3*	Data Trustworthiness: Specific

Security ID	Security Requirement	CTI 4501 ID	User Need or Functional Requirement
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.3.1	Data Sources: Resilience
		5.4.4.3.3	Data Processing: Resilience
6.3.4.2.14	Secure Communications: Other Users of External Data Entities for Which Checks Have Failed	5.4.4.1.3*	Data Trustworthiness: Specific
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.3.1	Data Sources: Resilience
		5.4.4.3.3	Data Processing: Resilience
6.3.4.2.15	Entitlement to Authentication Credentials	5.4.4.1.3*	Data Trustworthiness: Specific
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.2.16	Secure Issuance of Authentication Credentials	5.4.4.1.3*	Data Trustworthiness: Specific
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.2.17	Secure Re-Issuance of Authentication Credentials	5.4.4.1.3*	Data Trustworthiness: Specific
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.2.18	Blocking Re-Issuance of Authentication Credentials	5.4.4.1.3*	Data Trustworthiness: Specific
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.2.19	List of Privacy-Sensitive Information Flows	5.4.4.1.3*	Data Trustworthiness: Specific
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.2.20	Protecting Privacy-Sensitive Information Flows	5.4.4.1.3*	Data Trustworthiness: Specific
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.2.21	Protecting Sent Privacy-Sensitive Information when Received	5.4.4.1.3*	Data Trustworthiness: Specific
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
6.3.4.2.22	Security Size Overhead	5.4.4.1.3*	Data Trustworthiness: Specific
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.6.1	Security Performance: Size
		6.3.3.1.3.1	Transport Message Size - WAVE
6.3.4.2.23	Security Processing Overhead	5.4.4.1.3*	Data Trustworthiness: Specific
		5.4.4.2.2	Assurance of Trustworthiness of Messages Sent From CI
		5.4.4.6.2	Security Performance: Latency
	Protection of Cryptographic Keying Material: General		
	Protection of Cryptographic Keying Material: Hardware		
	Protection of Cryptographic Keying Material: Access to and Use of Keys		
6.3.4.3.1	TSC Infrastructure Protection: Invalid Signal Timing Information	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.1	Signal Timing Data Trustworthiness
		5.4.4.1.3.2	Signal Timing Status Trustworthiness
		5.4.4.1.3.9	Intersection Status Trustworthiness
		5.4.4.1.3.10	Current Movement State Trustworthiness
		5.4.4.1.3.11	Next Movement State Trustworthiness
		5.4.4.1.3.12	Time Change Details Trustworthiness

Security ID	Security Requirement	CTI 4501 ID	User Need or Functional Requirement
		5.4.4.1.3.13	Next Allowed Movement Time Trustworthiness
		5.4.4.1.3.14	Enabled Lanes Trustworthiness
		5.4.4.1.3.15	Signal Timing and Roadway Indications Synchronization Trustworthiness: Robustness
		5.4.4.1.3.16	Signal Timing and Roadway Indications Synchronization Trustworthiness: Correct Information
		CTI 4501/1: 6.3.2.1.1*	SPaT Information Requirements*
		CTI 4501/1: 6.3.2.2*	Signal Timing Status Requirements *
		CTI 4501/1: 6.3.3.1.2.1	Broadcast SPaT Message
6.3.4.3.2	TSC Infrastructure Protection: Invalid Format for Signal Timing Information	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.1	Signal Timing Data Trustworthiness
		5.4.4.1.3.2	Signal Timing Status Trustworthiness
		5.4.4.1.3.9	Intersection Status Trustworthiness
		5.4.4.1.3.10	Current Movement State Trustworthiness
		5.4.4.1.3.11	Next Movement State Trustworthiness
		5.4.4.1.3.12	Time Change Details Trustworthiness
		5.4.4.1.3.13	Next Allowed Movement Time Trustworthiness
		5.4.4.1.3.14	Enabled Lanes Trustworthiness
		5.4.4.1.3.15	Signal Timing and Roadway Indications Synchronization Trustworthiness: Robustness
		5.4.4.1.3.16	Signal Timing and Roadway Indications Synchronization Trustworthiness: Correct Information
6.3.4.3.3	TSC Infrastructure Protection: Incorrect Format for Signal Timing Information	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.1	Signal Timing Data Trustworthiness
		5.4.4.1.3.2	Signal Timing Status Trustworthiness
		5.4.4.1.3.9	Intersection Status Trustworthiness
		5.4.4.1.3.10	Current Movement State Trustworthiness
		5.4.4.1.3.11	Next Movement State Trustworthiness
		5.4.4.1.3.12	Time Change Details Trustworthiness
		5.4.4.1.3.13	Next Allowed Movement Time Trustworthiness
		5.4.4.1.3.14	Enabled Lanes Trustworthiness
		5.4.4.1.3.15	Signal Timing and Roadway Indications Synchronization Trustworthiness: Robustness
		5.4.4.1.3.16	Signal Timing and Roadway Indications Synchronization Trustworthiness: Correct Information
6.3.4.3.4	TSC Infrastructure Protection: Invalid Contents for Signal Timing Data	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.1	Signal Timing Data Trustworthiness
		5.4.4.1.3.2	Signal Timing Status Trustworthiness
		5.4.4.1.3.9	Intersection Status Trustworthiness
		5.4.4.1.3.10	Current Movement State Trustworthiness
		5.4.4.1.3.11	Next Movement State Trustworthiness
		5.4.4.1.3.12	Time Change Details Trustworthiness
		5.4.4.1.3.13	Next Allowed Movement Time Trustworthiness
		5.4.4.1.3.14	Enabled Lanes Trustworthiness
		5.4.4.1.3.15	Signal Timing and Roadway Indications Synchronization Trustworthiness: Robustness

Security ID	Security Requirement	CTI 4501 ID	User Need or Functional Requirement
		5.4.4.1.3.16	Signal Timing and Roadway Indications Synchronization Trustworthiness: Correct Information
6.3.4.3.5	Information About Availability of SPaT Information	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.1	Signal Timing Data Trustworthiness
		5.4.4.1.3.2	Signal Timing Status Trustworthiness
		5.4.4.1.3.9	Intersection Status Trustworthiness
		5.4.4.1.3.10	Current Movement State Trustworthiness
		5.4.4.1.3.11	Next Movement State Trustworthiness
		5.4.4.1.3.12	Time Change Details Trustworthiness
		5.4.4.1.3.13	Next Allowed Movement Time Trustworthiness
		5.4.4.1.3.14	Enabled Lanes Trustworthiness
		5.4.4.1.3.15	Signal Timing and Roadway Indications Synchronization Trustworthiness: Robustness
		5.4.4.1.3.16	Signal Timing and Roadway Indications Synchronization Trustworthiness: Correct Information
6.3.4.4.1	Validate Security of Approaching Vehicle V2X Messages	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.3	Approaching Vehicle Information Trustworthiness: RSU
		CTI 4501/1: 6.3.2.4.1	Receive BSM Messages
6.3.4.4.2	Validate Approaching Vehicle V2X Messages: Replay	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.3	Approaching Vehicle Information Trustworthiness: RSU
6.3.4.4.3	Validate Approaching Vehicle V2X Messages: Misbehavior Detection	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.3	Approaching Vehicle Information Trustworthiness: RSU
6.3.4.4.4	Validate Approaching Vehicle V2X Messages: Misbehavior Reporting	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.3	Approaching Vehicle Information Trustworthiness: RSU
6.3.4.4.5	Validate Approaching Vehicle V2X Messages: Distinguish Between Senders	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.3	Approaching Vehicle Information Trustworthiness: RSU
6.3.4.4.6	Security for Use of RSU BSM Filtering for RDZ	CTI 4501/1: 6.3.2.4.3	BSM Message Rate for AGP and RLVW
6.3.4.4.7	Security for Configuration of RSU BSM Filtering for RDZ	?	
6.3.4.5.1	Protection from Unnecessary AGP	CTI 4501/1: 6.3.2.3.2.1	Support AGP
6.3.4.6.1	Availability of Time Sources	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.5	Time Source Trustworthiness
		5.4.4.1.3.7	Timestamp Trustworthiness
		6.3.3.2.1	Time Accuracy
6.3.4.6.2	Detect Time Source Delay	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.5	Time Source Trustworthiness

Security ID	Security Requirement	CTI 4501 ID	User Need or Functional Requirement
		5.4.4.1.3.7	Timestamp Trustworthiness
6.3.4.6.3	Manage Time Source Delay	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.5	Time Source Trustworthiness
		5.4.4.1.3.7	Timestamp Trustworthiness
6.3.4.6.4	Time Source Delay for External Time Sources	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.5	Time Source Trustworthiness
		5.4.4.1.3.7	Timestamp Trustworthiness
6.3.4.6.5	Time Source Delay for External Time Sources: Other Users	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.5	Time Source Trustworthiness
		5.4.4.1.3.7	Timestamp Trustworthiness
6.3.4.7.1	List of CI Data Entities that Affect SPaT Contents	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.6	Message Revision Trustworthiness
		5.4.4.1.3.8	Intersection Identifier Trustworthiness
		5.4.4.1.3.9	Intersection Status Trustworthiness
		5.4.4.1.3.10	Current Movement State Trustworthiness
		5.4.4.1.3.11	Next Movement State Trustworthiness
		5.4.4.1.3.12	Time Change Details Trustworthiness
		5.4.4.1.3.13	Next Allowed Movement Time Trustworthiness
		5.4.4.1.3.14	Enabled Lanes Trustworthiness
		5.4.4.1.3.15	Signal Timing and Roadway Indications Synchronization Trustworthiness: Robustness
		5.4.4.1.3.16	Signal Timing and Roadway Indications Synchronization Trustworthiness: Correct Information
		CTI 4501/1: 6.3.3.1.1.1	SPaT Message - SAE J2735
		CTI 4501/1: 6.3.3.1.1.2	SPaT Message - Mandatory Data Elements
		CTI 4501/1: 6.3.3.1.1.3	SPaT Message - Required Data Elements
		CTI 4501/1: 6.3.3.1.1.4	SPaT Message PSID
		CTI 4501/2: 6.3.3.1.1.5	MAP Message - SAE J2735
		CTI 4501/1: 6.3.3.2.2.1	SPaT Message - Revision Counter Increment
		CTI 4501/1: 6.3.3.2.2.2	SPaT Message - Revision Counter Not Increment
		CTI 4501/1: 6.3.3.2.3*	Timestamp Requirements *
		CTI 4501/1: 6.3.3.3*	Signal Timing Data Requirements *
		CTI 4501/2: 6.3.3.4.4.2	Connection Egress Lane
		CTI 4501/2: 6.3.3.4.4.3	Connection Maneuvers
		CTI 4501/2: 6.3.3.4.4.4	Connection Signal Group
		CTI 4501/2: 6.3.3.4.4.5	Include Only Permitted Connections
6.3.4.7.2	Prevent Invalid SPaT Contents or Behavior	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.6	Message Revision Trustworthiness
		5.4.4.1.3.8	Intersection Identifier Trustworthiness

Security ID	Security Requirement	CTI 4501 ID	User Need or Functional Requirement
		5.4.4.1.3.9	Intersection Status Trustworthiness
		5.4.4.1.3.10	Current Movement State Trustworthiness
		5.4.4.1.3.11	Next Movement State Trustworthiness
		5.4.4.1.3.12	Time Change Details Trustworthiness
		5.4.4.1.3.13	Next Allowed Movement Time Trustworthiness
		5.4.4.1.3.14	Enabled Lanes Trustworthiness
		5.4.4.1.3.15	Signal Timing and Roadway Indications Synchronization Trustworthiness: Robustness
		5.4.4.1.3.16	Signal Timing and Roadway Indications Synchronization Trustworthiness: Correct Information
		CTI 4501/1: 6.3.3.1.6.1	Completeness - SPaT Message
		CTI 4501/1: 6.3.3.1.6.3	SPaT Message - Time Mark Accuracy
6.3.4.7.3	Detect Inconsistency of SPaT and Signal Timing Data	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.15	Signal Timing and Roadway Indications Synchronization Trustworthiness: Robustness
		5.4.4.1.3.16	Signal Timing and Roadway Indications Synchronization Trustworthiness: Correct Information
		5.4.4.4.2	Diagnostics For Incorrect Operations
6.3.4.7.4	Manage Inconsistency of SPaT and Signal Timing Data	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.15	Signal Timing and Roadway Indications Synchronization Trustworthiness: Robustness
		5.4.4.1.3.16	Signal Timing and Roadway Indications Synchronization Trustworthiness: Correct Information
6.3.4.8.1	List of CI Data Entities that Affect MAP Contents	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.6	Message Revision Trustworthiness
		5.4.4.1.3.8	Intersection Identifier Trustworthiness
		5.4.4.1.3.17	Intersection Geometry Trustworthiness
		5.4.4.1.3.18	Lane Attributes Trustworthiness
		5.4.4.1.3.19	Allowed Maneuvers Trustworthiness
		5.4.4.1.3.20	Connections Between Lanes Trustworthiness
		5.4.4.1.3.21	Approach Speed Limits Trustworthiness
		5.4.4.1.3.22	Revocable Lanes Trustworthiness
		5.4.4.1.3.23	Road Geometry Accuracy Trustworthiness
		5.4.4.1.3.24	Signal Timing and Roadway Geometry Synchronization Trustworthiness
		CTI 4501/2: 6.3.3.1.1.6	MAP Message - Mandatory Data Elements
		CTI 4501/2: 6.3.3.1.1.7	MAP Message - Required Data Elements
		CTI 4501/2: 6.3.3.1.1.8	MAP Message PSID
		CTI 4501/2: 6.3.3.1.3.2*	Concise MAP Message Requirements *
		CTI 4501/2: 6.3.3.4.1*	Intersection Geometry Requirements *
		CTI 4501/2: 6.3.3.4.2*	Lane Attributes *
		CTI 4501/2: 6.3.3.4.3	Lane Maneuvers

Security ID	Security Requirement	CTI 4501 ID	User Need or Functional Requirement
		CTI 4501/2: 6.3.3.4.4.1	Lane Connections
		CTI 4501/2: 6.3.3.4.5*	Speed Limit Information Requirements *
		CTI 4501/2: 6.3.3.4.6	Revocable Lanes
6.3.4.8.2	Prevent Invalid MAP Contents or Behavior	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.6	Message Revision Trustworthiness
		5.4.4.1.3.8	Intersection Identifier Trustworthiness
		5.4.4.1.3.17	Intersection Geometry Trustworthiness
		5.4.4.1.3.18	Lane Attributes Trustworthiness
		5.4.4.1.3.19	Allowed Maneuvers Trustworthiness
		5.4.4.1.3.20	Connections Between Lanes Trustworthiness
		5.4.4.1.3.21	Approach Speed Limits Trustworthiness
		5.4.4.1.3.22	Revocable Lanes Trustworthiness
		5.4.4.1.3.23	Road Geometry Accuracy Trustworthiness
		5.4.4.1.3.24	Signal Timing and Roadway Geometry Synchronization Trustworthiness
		CTI 4501/2: 6.3.3.1.6.2	Completeness - MAP Message
		CTI 4501/2: 6.3.3.2.2.3	MAP Message - Revision Counter Increment
		CTI 4501/2: 6.3.3.2.2.4	MAP Message - Revision Counter Not Increment
		CTI 4501/2: 6.3.3.2.2.5	MAP Message - Intersection Revision Counter Increment
		CTI 4501/2: 6.3.3.2.2.6	MAP Message - Intersection Revision Counter Not Increment
		CTI 4501/2: 6.3.3.3.2.11	Recent MAP Update
		CTI 4501/2: 6.3.3.3.2.12	New Lane IDs
6.3.4.8.3	External MAP Message Generation or Partial Generation: Data Source	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.17	Intersection Geometry Trustworthiness
		5.4.4.1.3.18	Lane Attributes Trustworthiness
		5.4.4.1.3.19	Allowed Maneuvers Trustworthiness
		5.4.4.1.3.20	Connections Between Lanes Trustworthiness
		5.4.4.1.3.21	Approach Speed Limits Trustworthiness
		5.4.4.1.3.22	Revocable Lanes Trustworthiness
		5.4.4.1.3.23	Road Geometry Accuracy Trustworthiness
		5.4.4.1.3.24	Signal Timing and Roadway Geometry Synchronization Trustworthiness
6.3.4.8.4	Prevent Inconsistency of MAP and Road Geometry or Use: False Positives	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.17	Intersection Geometry Trustworthiness
		5.4.4.1.3.18	Lane Attributes Trustworthiness
		5.4.4.1.3.19	Allowed Maneuvers Trustworthiness
		5.4.4.1.3.20	Connections Between Lanes Trustworthiness
		5.4.4.1.3.21	Approach Speed Limits Trustworthiness
		5.4.4.1.3.22	Revocable Lanes Trustworthiness
		5.4.4.1.3.23	Road Geometry Accuracy Trustworthiness
		5.4.4.1.3.24	Signal Timing and Roadway Geometry Synchronization Trustworthiness
		5.4.4.4.2	Diagnostics For Incorrect Operations
6.3.4.8.5	Prevent Inconsistency of MAP and Road Geometry or Use: False Negatives	5.4.4.1.1	Data Trustworthiness: Sources

Security ID	Security Requirement	CTI 4501 ID	User Need or Functional Requirement
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.17	Intersection Geometry Trustworthiness
		5.4.4.1.3.18	Lane Attributes Trustworthiness
		5.4.4.1.3.19	Allowed Maneuvers Trustworthiness
		5.4.4.1.3.20	Connections Between Lanes Trustworthiness
		5.4.4.1.3.21	Approach Speed Limits Trustworthiness
		5.4.4.1.3.22	Revocable Lanes Trustworthiness
		5.4.4.1.3.23	Road Geometry Accuracy Trustworthiness
		5.4.4.1.3.24	Signal Timing and Roadway Geometry Synchronization Trustworthiness
6.3.4.8.6	Detect Inconsistency of MAP and Road Geometry or Use	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.17	Intersection Geometry Trustworthiness
		5.4.4.1.3.18	Lane Attributes Trustworthiness
		5.4.4.1.3.19	Allowed Maneuvers Trustworthiness
		5.4.4.1.3.20	Connections Between Lanes Trustworthiness
		5.4.4.1.3.21	Approach Speed Limits Trustworthiness
		5.4.4.1.3.22	Revocable Lanes Trustworthiness
		5.4.4.1.3.23	Road Geometry Accuracy Trustworthiness
		5.4.4.1.3.24	Signal Timing and Roadway Geometry Synchronization Trustworthiness
6.3.4.8.7	Manage Inconsistency of MAP and Road Geometry or Use	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.17	Intersection Geometry Trustworthiness
		5.4.4.1.3.18	Lane Attributes Trustworthiness
		5.4.4.1.3.19	Allowed Maneuvers Trustworthiness
		5.4.4.1.3.20	Connections Between Lanes Trustworthiness
		5.4.4.1.3.21	Approach Speed Limits Trustworthiness
		5.4.4.1.3.22	Revocable Lanes Trustworthiness
		5.4.4.1.3.23	Road Geometry Accuracy Trustworthiness
		5.4.4.1.3.24	Signal Timing and Roadway Geometry Synchronization Trustworthiness
6.3.4.9.1	List of CI Data Entities that Affect RTCM Contents	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.6	Message Revision Trustworthiness
		5.4.4.1.3.25	RTK Corrections Message Trustworthiness
		J3258: 6.1.1	RTCMcorrections Message - SAE J2735
		J3258: 6.4	Real-Time Kinematics Requirements*
6.3.4.9.2	Prevent Invalid RTCM Contents or Behavior	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.6	Message Revision Trustworthiness
		5.4.4.1.3.25	RTK Corrections Message Trustworthiness
		J3258: 6.2.1	RTCMcorrections Message - Sequence Number Increment
6.3.4.9.3	External RTCM Message Generation or Partial Generation: Data Source	5.4.4.1.1	Data Trustworthiness: Sources
		5.4.4.1.2	Data Trustworthiness: Processing
		5.4.4.1.3.25	RTK Corrections Message Trustworthiness
6.3.4.10.1	SPaT and MAP Version Consistency	5.4.4.1.3.6	Message Revision Trustworthiness
		5.4.4.1.3.24	Signal Timing and Roadway Geometry Synchronization Trustworthiness
		CTI 4501/1: 6.3.3.4.7.1	Matching SPaT and MAP Version
6.3.4.10.2	SPaT and MAP Intersection Identifier Consistency	5.4.4.1.3.24	Signal Timing and Roadway Geometry Synchronization Trustworthiness
		CTI 4501/1: 6.3.3.4.7.2	Matching Intersection Reference Identifiers

Security ID	Security Requirement	CTI 4501 ID	User Need or Functional Requirement
6.3.4.11.1	Correctness of SPaT Availability Indications	CTI 4501/1: 6.3.3.3.2.14	No SPaT Available
6.3.4.11.2	Correctness of SPaT Unavailability Indications	CTI 4501/1: 6.3.3.3.2.14	No SPaT Available
6.3.4.11.3	Correctness of MAP Availability Indications	CTI 4501/1: 6.3.3.3.2.13	No MAP Available
6.3.4.11.4	Correctness of MAP Unavailability Indications	CTI 4501/1: 6.3.3.3.2.14	No SPaT Available
6.3.4.12.1	Robustness of Intersection Identifier Assignment	5.4.4.1.3.8	Intersection Identifier Trustworthiness
6.3.4.12.2	Detect Incorrect Intersection Identifiers	5.4.4.1.3.8	Intersection Identifier Trustworthiness
6.3.4.12.3	Manage Incorrect Intersection Identifiers	5.4.4.1.3.8	Intersection Identifier Trustworthiness
6.3.4.12.4	Detect Duplicate Use of Intersection Identifiers by External Parties	5.4.4.1.3.8	Intersection Identifier Trustworthiness
6.3.4.12.5	Manage Duplicate Use of Intersection Identifiers by External Parties	5.4.4.1.3.8	Intersection Identifier Trustworthiness
6.3.4.13.1	System Recovery - Software and Configuration Backups	5.4.4.3.2	Data Sources: Recovery
		5.4.4.3.4	Data Processing: Recovery
6.3.4.13.2	List of Operator-Notifiable Events	5.4.4.3.2	Data Sources: Recovery
		5.4.4.3.4	Data Processing: Recovery
6.3.4.13.3	List of Systemic Failure Events	5.4.4.3.2	Data Sources: Recovery
		5.4.4.3.4	Data Processing: Recovery
6.3.4.13.4	Cyberattack Must be Addressed	5.4.4.3.2	Data Sources: Recovery
		5.4.4.3.4	Data Processing: Recovery
6.3.4.13.5	Recovery Plan from Systemic Failure	5.4.4.3.2	Data Sources: Recovery
		5.4.4.3.4	Data Processing: Recovery
6.3.4.13.6	Recovery from Systemic Failure Only When Necessary	5.4.4.3.2	Data Sources: Recovery
		5.4.4.3.4	Data Processing: Recovery
6.3.4.13.7	Preserve Access Control During Systemic Failure	5.4.4.3.2	Data Sources: Recovery
		5.4.4.3.4	Data Processing: Recovery
6.3.4.13.8	Robustness of Recovery from Systemic Failure	5.4.4.3.2	Data Sources: Recovery
		5.4.4.3.4	Data Processing: Recovery
6.3.4.13.9	Assurance of Recovery from Systemic Failure	5.4.4.3.2	Data Sources: Recovery
		5.4.4.3.4	Data Processing: Recovery
6.3.4.13.10	Source Assurance for Recovery from Failure for Internal Data Sources or Processors	5.4.4.3.2	Data Sources: Recovery
		5.4.4.3.4	Data Processing: Recovery
6.3.4.13.11	Automated Recovery from Failure for the CI is not to be an Attack Vector	5.4.4.3.2	Data Sources: Recovery
		5.4.4.3.4	Data Processing: Recovery
6.3.4.13.12	Vulnerability Management for Potential	5.4.4.3.2	Data Sources: Recovery
		5.4.4.3.4	Data Processing: Recovery
6.3.4.13.13	Security Validation	5.4.4.3.2	Data Sources: Recovery
		5.4.4.3.4	Data Processing: Recovery
		6.3.5.3.5	Perform Validation
6.3.4.13.14	Access Control on Internal CI Data Entities During Life Cycle	5.4.4.5.2*	Life Cycle Security Needs *
6.3.4.13.15	Maintenance Security Needs	5.4.4.5.3	Maintenance Security Needs
		6.3.5.2.1	Documented Plan for Life Cycle Operations & Maintenance
	Security Knowledge for Personnel		
6.3.4.14.1	CI Performance Monitoring System	5.4.4.4.3	Confidential Information Within Diagnostics Systems
		5.4.4.4.4	Correct Information Within Diagnostics System
		5.4.4.4.5	Confidential Information Within Performance Monitoring Systems

Security ID	Security Requirement	CTI 4501 ID	User Need or Functional Requirement
		5.4.4.4.6	Correct Information Within Performance Monitoring Systems
6.3.4.14.2	Events to be Monitored by	5.4.4.4.1	Diagnostics for Security Issues
6.3.4.14.3	CPMS: Other System Monitoring	?	
6.3.4.14.4	CPMS: Robustness Against Invalid Input	?	
6.3.4.14.5	CPMS: Error Management	5.4.4.3.2	Data Sources: Recovery
		5.4.4.3.4	Data Processing: Recovery
6.3.4.15.1	Prevent Unauthorized CI Software and Configuration Changes	5.4.4.5.4.1	Upgrade System: Correct Operation
6.3.4.15.2	Authenticate and Verify Integrity of All Software/Firmware Updates	5.4.4.5.4.1	Upgrade System: Correct Operation
6.3.4.15.3	CI Data Entity Update: Validation	5.4.4.5.4.1	Upgrade System: Correct Operation
6.3.4.15.4	CI Data Entity Update: Correct Status	5.4.4.5.4.2	Upgrade System: Correct Status
6.3.4.15.5	Tracking Evolution of CI-Related Standards	5.4.4.5.1	Security Interoperability
6.3.4.15.6	Tracking of Installed Version Information to CI-Related Standards	5.4.4.5.1	Security Interoperability
6.3.4.15.7	Update Cadence of CI Systems to CI-Related Standards		
6.3.4.16.1	Correct Operational Mode Protection	6.3.5.3.1	Support Normal Mode
		6.3.5.3.2	Maintenance Mode
		6.3.5.3.4	Support Maintenance Mode Fallback
		6.3.5.3.6	Command Maintenance Mode
		6.3.5.3.7	Automatic Return to Normal Mode
		6.3.5.5.2	Support Maintenance Mode in Monitoring
6.3.4.16.2	Correct Mode and Status Reporting	6.3.5.3.3	Report Operational Mode Status
6.3.4.16.3	Protection Against Improper Operation in Maintenance Mode	?	
6.3.4.16.4	Protecting Determinations that Normal Mode Transition Criteria are Met	?	
6.3.4.16.5	Correct Representation of Operating Mode	?	
6.3.4.17.1	Prevent Change in Data Coverage		
6.3.4.17.2	Detect Change in Data Coverage		
6.3.4.17.3	Prevent Change in Radio Power		
6.3.4.17.4	Detect Change in Radio Power		
6.3.4.18	CI Security Verification Requirements		