

Enabling Trust and Deployment Through Verified Connected Intersections

Strengthening Mobility and Revolutionizing Transportation (SMART)
Grants Program – FY2022 Award to Utah Department of Transportation
(Period of Performance: July 15, 2023 – August 30, 2025)

Final Implementation Report

Prepared by: **Athey Creek Consultants** on behalf of the
Utah Department of Transportation

In partnership with: **Crash Avoidance Metrics Partners (CAMP), LLC** and
Security Credential Management System (SCMS) Manager, LLC

August 30, 2025



1. Executive Summary

This document summarizes the findings of the Utah Department of Transportation (UDOT) Strengthening Mobility and Revolutionizing Transportation (SMART) Grant Stage 1 effort, supported by the United States Department of Transportation (USDOT), entitled *Enabling Trust and Deployment Through Verified Connected Intersections*. The primary objective of this effort was to establish mechanisms whereby original equipment manufacturers (OEMs) can trust that connected intersection (CI) broadcasts are accurate, consistent, reliable, and secure, based on requirements in Connected Transportation Interoperability (CTI) 4501 and processes defined by Security Credential Management System (SCMS) Manager, in order to facilitate large-scale connected vehicle (CV) deployment, by achieving the following goals:

- Complete a successful reference implementation corridor in the Salt Lake City metro area.
- Develop a process and credentialing guidance for OEMs to trust CIs to have accurate, consistent, reliable, secure messages.
- Establish ongoing collaboration between Infrastructure Owner Operators (IOOs), OEMs, and SCMS Manager and providers.
- Conduct targeted outreach and work with other deploying IOOs.
- Make test tools, procedures, validation processes, and policies publicly available and/or refer to reports and deliverables published by established standards bodies, such as SAE, and other organizations.

The project partners included UDOT, OEMs participating in the Crash Avoidance Metrics Partners Limited Liability Company (CAMP LLC) "Model Deployment of Connected and Automated Mobility" Consortium, and SCMS Manager. Overall, the testing tools and software developed in this effort to validate CIs work and demonstrated success at identifying where requirements were not met, allowing the UDOT Project Team to address issues identified. Additionally, user guides and resources were developed as a part of this effort to help users collect CI data, use the developed tools, and follow the developed CI validation approach. While stated project goals and outcomes were not entirely achieved, considerable progress was made towards validating CIs along a corridor and the project identified issues that need to be addressed to achieve a fully validated corridor. This effort successfully demonstrated that further expansion to at-scale implementation is feasible, and more agency experiences are needed to better understand the scalability and long-term impacts of operating and maintaining validated CIs. The tools, procedures, and overall data collection and analysis process developed in this effort are now available and recommended for use by other IOOs in order to further refine and enhance them based on new experiences and lessons learned as part of at-scale implementation.

2. Introduction and Project Overview

Connected vehicle (CV) technology offers the promise of fewer crashes and fatalities, increased efficiency, and environmental improvements. At signalized intersections with CV technology, referred to as Connected Intersections (CIs), infrastructure-based vehicle-to-everything (V2X) devices broadcast messages about the intersection status (i.e., Signal Phase and Timing (SPaT) message, MAP message containing intersection geometry information, and Radio Technical Commission for Maritime Services (RTCM) message for position correction information). Information broadcast by CIs is received by in-vehicle V2X devices, where applications process the information and warn drivers if warranted by the conditions. For the purposes of this effort, V2X devices are broadcasting messages within the 5.9 GHz spectrum using roadside units (RSUs) for low-latency CV safety applications; however, other applications and V2X devices may also or only use network cellular communications.

Several groups have made significant progress on CI standards in the past three years. The United States Department of Transportation (USDOT), through the Institute of Transportation Engineers (ITE) Connected Intersections effort developed the *Connected Transportation Interoperability (CTI) 4501 CI Implementation Guide*¹, and the Connected Vehicle Pooled Fund Study (CV PFS), a group of 22 Federal, State, local, and international transportation agencies has advanced a variety of CI efforts. The CI standards are based on the Red-Light Violation Warning (RLVW) application, a key safety application being prepared for early deployment in equipped vehicles. Note that USDOT is funding a CTI CI Phase 2 effort that is being led by SAE to expand on this work and update the CTI 4501 standard, which is expected to be published in 2025.

2.1 Project Description

For twenty years, CV applications have offered a promise of fewer crashes and fatalities, increased efficiency, and environmental improvements. After several years of regulatory uncertainty, the CV promise is on the brink of being brought to reality, if industry can overcome the remaining hurdles, which this effort sought to do. Specifically, this effort sought to establish mechanisms whereby original equipment manufacturers (OEMs) can trust that CI broadcasts are accurate, consistent, reliable, and secure, based on requirements in CTI 4501 and processes defined by Security Credential Management System (SCMS) Manager, in order to facilitate large-scale CV deployment.

Motivation

The motivation for this project was to set the foundation for confronting real-world challenges to be addressed by at-scale implementation of CIs. The specific challenge this project addressed was that at the completion of the aforementioned USDOT-funded CTI CI Phase 2 project, the automotive industry would still lack a mechanism to trust that Infrastructure Owner-Operator (IOO) deployed CIs are broadcasting accurate, consistent, reliable, and secured messages needed to support in-vehicle RLVW and other safety applications. Without a reproducible process to validate intersections, a coupling of this validation process to the issuance of security credentials (to inform the vehicle that the intersection has been validated), a process for detecting and reporting misbehavior and re-testing intersections, and a field deployment demonstrating validated broadcasts, production vehicles with these life-saving applications are unable to operate.

Technologies

Deliverables this project advanced and outcomes of this project included:

- Technologies. Existing hardware and software at UDOT intersections that were already equipped as CIs were tested, refined, and improved, as needed, to meet requirements established by the USDOT-funded CTI 4501 Phase 2 effort and expectations of project partners;

¹ Institute of Traffic Engineers. *Connected Transportation Interoperability (CTI) 4501 v01.01 Connected Intersections Implementation Guide*. Last accessed Sept 2023:
<https://www.ite.org/ITEORG/assets/File/Standards/CTI%204501v0101.pdf>

- Test Tools and Processes. Test tools comprised of a combination of hardware and software were specified and developed in this project to be used to validate that CIs meet the expectations of project-participating OEMs and SCMS Manager; and
- Validation Process. An overall validation process and credentialing policy that utilizes the testing tools developed in this project and supporting tools developed by the CV PFS were developed by SCMS Manager and implemented in Utah during this Stage 1 effort. The creation and demonstration of this process and policy can be used to help other IOOs understand the implications (e.g., necessity, time commitment and costs) to perform validations at their locations.

Goals

The CIs completed and validated under this planning and prototype stage, as well as the CIs to be validated and trusted as a result of Stage 2 activities, will enable the eventual at-scale implementation of an underlying CI infrastructure to support in-vehicle safety applications to help reduce red-light running related crashes and other safety, mobility, and environmental applications. These impacts will benefit the entire community of drivers and riders in vehicles. The following bullets summarize the Stage 1 project goals as well as the statutory language in the Investment and Jobs Act (IIJA) (Public Law 117-58 Sec 25005) related to each:

1. Complete a successful reference implementation corridor. (IIJA: improve safety, improve reliability, increase resiliency, incentivize private-sector investments or partnerships)
2. Develop a process and credentialing guidance for OEMs to trust CIs to have accurate, consistent, reliable, secure messages. (IIJA: improve safety, improve reliability, private-sector investments or partnerships)
3. Establish ongoing collaboration between IOOs, OEMs, and SCMS Manager and providers. (IIJA: incentivize private-sector investments or partnerships)
4. Conduct targeted outreach and work with other deploying IOOs. (IIJA: improve safety, improve reliability)
5. Make test tools, procedures, validation processes, and policies publicly available and/or refer to reports and deliverables published by established standards bodies, such as SAE, and other organizations. (IIJA: improve safety, improve reliability)

Impacted Communities

Stage 1 efforts were very technically focused, so widespread public outreach and engagement was not conducted. However, limited outreach to CV PFS members and other IOOs was conducted. The ultimate safety benefits will be recognized by the entire community of the traveling public through expanded efforts and deployment in the future. The long-term vision is that CIs will be operational at the vast majority of the approximately 300,000 state and locally operated signalized intersections, as envisioned by the USDOT National V2X Deployment Plan, *Saving Lives with Connectivity*.²

While the CTI 4501 efforts were focused on RLVW, the requirements for accuracy, consistency, and reliability are relatively rigid compared with what may be required for other safety and mobility applications. Therefore, while the CTI 4501 efforts did not analyze other applications, it is anticipated that other safety and mobility related applications that OEMs may consider will be supported by CIs validated against CTI 4501 requirements.

² United States Department of Transportation. *Saving Lives with Connectivity: A Plan to Accelerate V2X Deployment*. Last accessed December 2024:
https://www.its.dot.gov/research_areas/emerging_tech/pdf/Accelerate_V2X_Deployment_final.pdf

2.2 Proof-of-Concept Overview

Scale of Stage 1 Deployment

The proof of concept assessed in this Stage 1 project was the creation of a validation process (and supporting tools and credentialing policy) that were intended to enable OEMs to trust that CIs deployed by IOOs are broadcasting accurate, consistent, reliable, and secured messages that can support in-vehicle RLWV and other CI related safety applications.

The focus of this effort for testing and validation was on a corridor that was already equipped with RSUs: SR-224 near Park City (a rural community) with Intelight controllers and Kapsch cellular-vehicle to everything (C-V2X).

Project Partners

The project partners included an IOO (i.e., UDOT), OEMs participating in the Crash Avoidance Metrics Partners Limited Liability Company (CAMP LLC) “Model Deployment of Connected and Automated Mobility” Consortium (referred to hereafter as CAMP), and SCMS Manager, however industry consensus extended beyond the project partners as part of outreach efforts to other entities for feedback, including the CV PFS for IOO inputs and participants in the USDOT-sponsored CTI Phase 2 effort for broader industry input.

Anticipated Scale of Stage 2 Deployment

This effort envisioned a Stage 2 “at-scale” effort that would expand the use of the validation process to more corridors in Utah, additional IOOs (at least six or more additional IOOs), and further engage OEMs and SCMS Manager to expand the validation process to accommodate increasing numbers of IOOs participating. Given the number of signalized intersections operated by local agencies, a Stage 2 at-scale deployment was envisioned to engage a number of IOOs that were local agencies, as well as state agencies (e.g., Georgia Department of Transportation (DOT), Arizona’s Maricopa County DOT, Texas Transportation Institute, University of Michigan Transportation Institute working in Ann Arbor, Ohio DOT, and Florida’s Tampa Hillsboro Expressway Authority) to facilitate the knowledge transfer and training activities from UDOT. A Stage 2 at-scale deployment would better support activities that remain new and evolving, such as the availability of a bench test environment and troubleshooting issues with signal controllers and configurations, test tools themselves, and other CV equipment as they arise. This Stage 2 “at-scale” deployment would increase IOO readiness for OEM introduction of RLWV and other safety applications in production vehicles and move the needle toward a critical mass of IOO operated intersections equipped to broadcast the data needed for lifesaving RLWV applications. One outcome of a Stage 2 deployment would be a better understanding of training needs to further expand the CI deployment, testing, and validation to other state and local IOOs around the country.

Key Barriers to CV Safety Application Deployment on Production Vehicles

Initial feedback from CAMP indicated that the key barriers remaining were:

- Confidence in data coming from CIs (overcome via tools and processes developed by this Stage 1 effort)
- Number of equipped and validated CIs (progress can be made through a Stage 2 effort and unrelated efforts like the USDOT Accelerating V2X Grant Program and other grant programs)
- Release of the second FCC report and order to ensure certainty (released in November 2024)

Factors impacting the scale of Stage 2 deployment include the costs to conduct testing and validation activities and the availability of products (e.g., signal controllers) that fully comply with CTI 4501 requirements for a fully validated intersection. These factors may impact the number of CIs that are able to be validated. Additionally, the November 2024 release of the Federal Communications Commission (FCC) Second Report and Order should bring additional certainty to this space and potentially expedite use of V2X technology in OEM production vehicles. In doing so, more IOOs may be willing to advance CI deployment.

Eventually, more broadly and over a longer term, deployment, testing, and validation of CIs will likely coincide with widespread deployment of in-vehicle CV safety applications by OEMs that rely upon the broadcasts of data from validated CIs. This is when the full “at-scale” benefits will be achieved.

This validation process is a key enabler for the USDOT National V2X Deployment Plan³ of having two vehicle OEMs commit to 5.9 GHz capable vehicles by the 2027 model year. Feedback from CAMP during this initiative indicated that three barriers to OEMs including V2X technologies in production vehicles are:

- Lack of trust in CI data,
- The number of validated CIs deployed, and
- The lack of a Second Report and Order from FCC (which was released in November 2024, near the conclusion of this effort).

2.3 Summary of Project Activities

Milestones

The milestones for this effort fell within six categories that were tracked through the course of the project:

1. **SPaT Validation.** The four milestones were to:
 - Build and test SPaT testing and evaluation tools.
 - Define pass/fail requirements for SPaT messages compared to CTI 4501 requirements.
 - Define test scenarios that any IOO can implement.
 - Conduct SPaT validation in Utah to demonstrate functionality and feasibility.
2. **MAP Validation.** Milestones were to:
 - Create a tool and, as needed, a supporting process to evaluate MAP accuracy to support other IOOs in validating CIs.
 - Enhance the MAP accuracy processing tool created in the ITE CTI 4501 Phase 1 project.
 - Conduct an initial test of the Light Detection and Ranging (LiDAR) road scan and post-processing tool assessing affordability and industry ability to meet the specification.
 - Modify the MAP evaluation and post-processing tool as needed and conduct further validation before encouraging widespread IOO use.
3. **RTCM Research and Possible Validation.** The key milestone was to explore the impacts of RTCM accuracy on vehicle positioning, and then, if needed, create an RTCM validation tool and conduct RTCM validation in Utah.
4. **Connected Intersection Message Monitoring System (CIMMS) Assessment for Ongoing Monitoring of Validated Intersections.**⁴ Two milestones were to:
 - Determine an approach for using CIMMS, developed by the CV PFS, as an ongoing monitoring tool to continuously validate that intersections meet some critical CTI 4501 requirements.
 - To assess the sensitivity of CIMMS reports and understand other functions for CIMMS (e.g., CIMMS as a possible initial test of MAP accuracy).
5. **SCMS Manager Policies and Procedures.** The two milestones were to:
 - Develop policies and procedures that SCMS providers can require IOOs operating CIs to follow when validating intersections, and then use the validation information to indicate within the security certificate that a CI has been validated.
 - Pilot and confirm the effectiveness and practicality of these in the Utah corridors.
6. **Overall Project Management.** Milestones included creating document sharing for the project team, completing updates on the Utah corridor, and considering a Stage 2 Grant Application.

³ Ibid (*Saving Lives with Connectivity: A Plan to Accelerate V2X Deployment*).

⁴ Connected Vehicle Pooled Fund Study. *Connected Intersection Message Monitoring System (CIMMS) Final Report*. Last accessed July 2024: <https://engineering.virginia.edu/labs-groups/cvpfs>

Project Attention

This effort has been discussed among industry professionals, in particular through discussions and presentations to CV PFS members and participants in CTI 4501 Phase 2 efforts.

Deviations from Original Plan

The original plan was to develop a corridor of verified CIs, and this was not accomplished. During the last round of testing and validation, the CIs were very close to being fully validated and the roadblocks that prevented achieving validation were aspects that are out of the control of the project team. Additionally, two additional corridors (i.e., US-89 in American Fork with Econolite controllers and Kapsch C-V2X RSUs and SR-68 (Redwood Road) in Salt Lake City with Intelight controllers and Commsignia C-V2X RSUs) were initially proposed for testing, however challenges with Econolite firmware updates and a determination by the project team that testing and validation efforts would yield similar results on these corridors as the SR-224 corridor led to a decision to not conduct additional testing on these two corridors.

2.4 Document Organization

The remainder of this document is oriented around the following six sections:

3. [Proof-of-Concept Evaluation Findings](#) presents the findings from the Utah proof of concept as they relate to each performance measure identified in the evaluation plan, as well as a narrative of how this effort met original expectations and demonstrated improvement in specific goal areas.
4. [Anticipated Costs and Benefits of At-Scale Implementation](#) describes the anticipated impacts and costs of at-scale implementation, as well as baseline data and the methods to estimate these impacts and costs for at-scale implementation.
5. [Challenges, Best Practices, and Recommendations](#) describes lessons learned and insights that may assist with future deployers with fully validating CIs in their jurisdictions.
6. [Deployment Readiness](#) summarizes the readiness of this effort for at-scale implementation and the remaining gaps in understanding the scalability and long-term impacts of operating and maintaining fully validated CIs.
7. [Wrap Up](#) reflects on the project to discuss whether the proposed solution met expectations, possible changes to the solution that should be made for at-scale implementation, and advice for others pursuing the solution.
8. [Terms and Acronyms](#) defines common items used in this document.

3. Proof-of-Concept Evaluation Findings

This section presents the findings from the Utah proof of concept. Note that this evaluation effort differed from a more traditional evaluation that focuses primarily on data analyses. While the testing and validation of the CIs conducted in this project relied on data comparisons to assess the accuracy, consistency, and reliability of the data broadcast by CIs, the primary purpose of this evaluation was not to assess the CI itself, but to assess the development, usability, and costs of implementing the validation processes and tools that key stakeholder participants (i.e., CAMP, SCMS Manager, and CV PFS IOOs) agreed were acceptable for nationwide CI deployment and V2X communications. In other words, success for this project was defined by an industry consensus and acceptance of the products that were developed, rather than specific details about the products themselves.

3.1 Findings on the Proof-of-Concept Performance

This subsection defines the performance measures from the evaluation plan, describes the data that was collected, and summarizes the findings. Note that all of the supporting resources developed as part of this effort are available on the UDOT Transportation Technology webpage at: <https://transportationtechnology.utah.gov/what-were-learning>; it should be noted that **these resources are expected to evolve in the near future as part of other efforts** including the UDOT SMART Stage 2 effort. Table 1 presents the findings for specific performance measures from the evaluation plan that were assessed.

Specific findings from the proof-of-concept included:

- The developed testing tools and software work and demonstrated success at identifying where CTI 4501 requirements were not met, allowing the UDOT Project Team to address issues identified. A reference guide of the data collection tool was developed by The Narwhal Group entitled *Traffic Signal Cabinet Logging Tool Quick Reference Guide*. The SPaT and MAP software and testing processes are respectively documented in three resources developed by CAMP entitled *Assessment of SPaT Accuracy to Support RLWV Application*, *Assessing Node Point Accuracy in the SAE J2735 MAP Message*, and *Validation Assessment & Analysis Software Toolset User Guide, Version 3.0*. Reporting expectations for test findings are documented in the *CI Test Results Report Format* resource developed by the SCMS provider Integrated Security Services (ISS) for this effort. The SPaT and MAP testing and validation tools are available at <https://portal.dm.preprod.v2x.isscms.com/login>; users may request access for free from ISS at: <https://www.ghsiss.com/v2x-certificates>. Additionally, Appendix A presents the errors identified during SPaT testing for RSUs procured from two different providers.
- A new MAP validation approach was introduced and included a developed specification for LiDAR data collection to be used as an input to the MAP assessment tool. This specification is included in the CAMP *Assessing Node Point Accuracy in the SAE J2735 MAP Message* resource. This validation approach was demonstrated using both existing and new LiDAR road scan data. Assessing the relative accuracy of any given LiDAR road scan (e.g., with a field survey) is a recommended activity for Stage 2 At-Scale Deployment.
- A new MAP validation tool was developed that assesses the accuracy of the MAP message against ground truth data (LiDAR data for purposes of this project) and provides recommended adjustments to nodes within the MAP message that would allow it to be validated. This new MAP validation tool is combined with the previous MAP validation tool (a product of the CTI activities) that tested MAP messages for completeness of data and proper formatting. The MAP validation tool is available at <https://portal.dm.preprod.v2x.isscms.com/login>; users may request access for free from ISS at: <https://www.ghsiss.com/v2x-certificates>.
- Feedback from OEMs in CAMP and SCMS Manager indicate that stated project goals and outcomes were not entirely achieved. The original goal was to develop a corridor of verified CIs, and this was not accomplished. However, considerable progress was made towards validating the CIs along the corridor and the project identified the issues that need to be addressed to achieve a validated corridor. During the last round of testing and validation, the intersections were very close

to being fully validated and the roadblocks that prevented achieving validation were aspects that are out of the control of the project team. Specifically, the data coming out of the signal controller does not, on occasion, represent the signal controller status, and there are occasional latency issues with the RSUs. Both of these will require updates or improvements from the manufacturers before these intermittent events can be avoided entirely. Appendix A includes a summary of the types of errors encountered. A final situation that prevented full validation of the corridor was uncertainty about whether RTCM messages are needed (i.e., could not verify RTCM message requirements in the reference implementation corridor as these have not yet been completed by the CTI 4501 effort), as described in more detail below.

- The focus of this effort for testing and validation was on a corridor that was already equipped with RSUs: SR-224 near Park City (a rural community) with Intelight controllers and Kapsch C-V2X. The data and the resulting analysis reports can be found on [Zenodo](#) via the [UDOT Transportation Technology Verifying Connected Intersections](#) webpage.^{5,6} Specifically, this dataset contains a series of folders for each tested CI in the reference implementation corridor, SR-224. A separate file for each tested CI contains the data collected at the CI for SPaT testing (described in the 2024 *Traffic Signal Cabinet Logging Tool Quick Reference Guide*) and the output reports from the SPaT validation tool (described in the 2024 *CAMP Assessment of SPaT Accuracy to Support RLVW Application* report), as well as the data collected at the CI for MAP testing and the output reports from the MAP validation tool (described in the 2024 *CAMP Assessing Node Point Accuracy in the SAE J2735 MAP Message* report).
- Two additional corridors (i.e., US-89 in American Fork with Econolite controllers and Kapsch C-V2X RSUs and SR-68 (Redwood Road) in Salt Lake City with Intelight controllers and Commsignia C-V2X RSUs) were initially proposed for testing, however challenges with Econolite firmware updates and a determination by the project team that testing and validation efforts would yield similar results on these corridors as the SR-224 corridor led to a decision to not conduct additional testing on these two corridors.
- Questions remain about how palatable the CI validation process and costs may be to IOOs, which was why developed validation processes were considered for affordability and palatability for not only State IOOs but also local city and county IOOs that ultimately must embrace these validation processes.
- Project activities achieved the desired outcomes specified by the project goals and analyzed per the performance measures identified in the Evaluation Plan. Project activities conducted in this proof-of-concept identified some new gaps or questions that will be explored and addressed as part of Stage 2 At-Scale Deployment activities.
- Resources developed as part of this effort are initial versions and are expected to be updated and evolve in the near future as part of other efforts, including the UDOT SMART Stage 2 effort. In particular, resources developed by SCMS Manager in this effort entitled *SCMS Manager Intersection Validation and Certificate Issuance Policy* and *SCMS Manager Intersection Validation Misbehavior Management* have not yet been implemented and future refinements are anticipated. Additional experience from the use of all resources developed in this effort will inform future updates to these documents.

Lessons learned that were identified included:

- Challenges were identified with MAP creation processes for full CTI 4501 compliance. For example, node point selection when creating a MAP message manually or with a creation tool is highly likely to result in errors that prevent a developed MAP from being accurate to CTI 4501 requirements. To address this challenge, the MAP validation tool developed in this project includes an output that identifies coordinates for alternate node points that are within the tolerance established by CTI 4501. However, refinements are needed to apply these outputs

⁵ Dataset archive link: <https://doi.org/10.5281/zenodo.16740843>.

⁶ Available at: <https://transportationtechnology.utah.gov/verifying-connected-intersections/>.

- Challenges were identified with time sources of signal controllers that cannot be resolved by the project team without updates from the signal control manufacturer.
- Challenges were identified with some preliminary requirements in the draft update to CTI 4501 that led to the development of a profile for testing by ISS with project team input, which is documented in the *CTI 4501 Security Policy Profile* resource.
- Tools developed in this effort identified very specific issues in signal controller manufacturer firmware (note that only Kapsch signal controllers were tested in this effort), as well as different issues with devices in different configurations. This pointed to a recognized need for a process to share findings with the signal controller manufacturers.
- A preferred MAP validation data source or collection approach was not readily identified in this effort. Additional analysis and evaluation is recommended as part of the Stage 2 At-Scale Deployment, and some manual interpretation may be required in the interim period.
- Developing the SPaT data collection device (e.g., using a Cohda on-board unit) was not as straightforward as anticipated because of some hardware and firmware constraints.

Table 1. Performance Measures and Findings of this Effort

Performance Measure from Evaluation Plan	Findings
Outcomes of testing and validation procedures and reactions from OEMs in CAMP and SCMS Manager that a fully validated corridor was achieved.	The implementation corridor was not able to consistently meet all CTI 4501 requirements for a fully validated intersection. Developed validation tools and processes worked, as expected; testing identified very specific issues in signal controller manufacturer firmware and other areas, confirming that the tools can fully validate a CI when issues beyond IOO control are resolved by manufacturers.
Feedback from UDOT and CV PFS members about whether the implementation corridor will help to reduce the time and costs to fully validate other CIs.	The implementation corridor was not able to consistently meet all CTI 4501 requirements for a fully validated intersection due to issues beyond IOO control. However, a profile (i.e., a subset of those requirements most critical to OEMs trusting intersections for RLVW application deployment) was completed and presented in the <i>SCMS Manager Intersection Validation and Certificate Issuance Policy</i> report, and can support other sites as they proceed with validating their corridors. If alternate approaches to capturing accurate lane line lat/lon values for the MAP message is identified in Stage 2, the Utah corridor can be used as a reference corridor to test these.
OEMs in CAMP can confirm they trust the process to validate CIs.	Developed validation tools and processes worked, as expected and are recognized by CAMP partners as trusted tools.
SCMS Manager confirms the testing procedures are acceptable to validate CIs.	Automated tool outputs and reports were acceptable to validate CIs.
Successful implementation by UDOT of the testing tools and procedures to test the reference implementation corridor.	Test tools and procedures were successfully used to test the reference implementation corridor.

Performance Measure from Evaluation Plan	Findings
Reactions from other IOOs about their knowledge of the project outcomes and the extent to which they are willing to perform the validation process on their CIs.	CV PFS Members were made aware of progress of this project in May 2024 and were updated in December on project outcomes. Several sites agreed to test and validate existing CIs as part of a Stage 2 At-Scale Deployment, demonstrating a willingness to perform the validation process.
Reported time and/or contractor expense performing the validation process in Stage 1.	Costs were recorded for the LiDAR data to validate MAP messages, data collection and testing per CI, and testing device equipment and assembly. (See Section 4.2)
Documentation of lessons learned and recommendations from UDOT, CAMP, and SCMS Manager to facilitate Stage 2 implementation.	Lessons learned were documented. (See Section 3.1)
Confirmation of tool availability.	Tools are available through SCMS provider ISS at: https://portal.dm.preprod.v2x.isscms.com/login ; users may request access for free at: https://www.ghsiss.com/v2x-certificates
Reaction from IOOs outside the project if they are able to access and use test tools.	Tools are available through SCMS provider ISS at: https://portal.dm.preprod.v2x.isscms.com/login ; users may request access for free at: https://www.ghsiss.com/v2x-certificates . Other IOOs have not yet used the test tools, but will be doing so as part of the SMART Stage 2 effort.
Valid procedure to protect integrity of data by only issuing valid SCMS certificates to fully validated CIs.	SCMS Manager Intersection Validation Misbehavior Management report defines the procedure developed by this project that identifies the profile of requirements that are most critical to fully validate a CI.
Reaction and feedback from UDOT, OEMs in CAMP, and SCMS Manager, and examples of the collaboration accomplished in this project.	Feedback collected from project team members on collaboration confirmed the collaboration has led to an approach that is acceptable to the CAMP partners, SCMS Manager, and UDOT and may be expanded or evolve as part of the SMART Stage 2 effort.

3.2 How This Proof-of-Concept Met Original Expectations and Goals

As indicated in Table 1, the proof-of-concept met original expectations and goals overall. At the beginning of this effort, despite several significant testing activities in Utah, a complete set of information was still not available to IOOs about what specifically was needed to fully achieve SCMS and OEM trust in their CIs, including what the process should consist of, the tools available, and estimated costs to accomplish it. Further, OEMs had concerns over the data broadcast by CIs, which was a barrier towards implementation of RLVW applications.

For this proof-of-concept, CAMP, SCMS Manager, Narwhal, and other project team members successfully collaborated to develop test tools and procedures that they agree can be used by IOOs to validate CIs. The tools have proven sufficiently robust for validating the selected UDOT CIs but also identified previously unknown issues in the signal controllers that ultimately require signal controllers to implement a software update to address properly. As such, the reference implementation corridor only meets CTI 4501 requirements that are achievable at the end of 2024 based on available technologies; outstanding issues will remain until software updates become available. Specifically, the UDOT CIs were tested to be a reference implementation corridor for a profile or subset of CI requirements following the procedure

developed as a part of this effort, as described in *SCMS Manager Intersection Validation and Certificate Issuance Policy*. However, the reference implementation corridor was not able to consistently meet all requirements for a fully validated intersection as part of these testing activities. Two key takeaways are:

1. This project produced robust validation tools and procedures that effectively identify issues and (when appropriate) validate CIs with no issues.
2. Where issues are identified, these may not be things that the IOO and supporting contractors can address and may require signal (or other equipment) manufacturers to address through new software releases. While this may introduce additional time for fully validating CIs against all CTI 4501 requirements, the software releases are expected to benefit other IOOs operating other CIs. Collectively, the industry will become more "CI friendly" over time.

3.3 How This Proof-of-Concept Demonstrated Improvement in Statutory Areas

The proof-of-concept demonstrated the following improvements in four areas identified in statutory language in the IIJA (Public Law 117-58 Sec 25005):

- Improve the **safety** and integration of transportation facilities and systems for pedestrians, bicyclists, and the broader traveling public;
- Improve the **reliability** of existing transportation facilities and systems;
- Incentivize private sector investments or **partnerships**, including by working with mobile and fixed telecommunication service providers, to the extent practicable; and
- Increase the **resiliency** of the transportation system.

Improve Safety and Improve Reliability

- The automated analyses of signal controller data and resulting SPaT messages resulted in very informative outputs, identifying rare occurrences of conflicts in the data. This demonstrated several key messages:
 - The tools and procedures work, and observations by OEM participants and SCMS Manager to this process increased their confidence that robust verification tools were being produced.
 - While always anticipated, coordination with signal control manufacturers became recognized as critical to understand why these rare data conflicts occur and to enable these and other manufacturers to solve the issues properly.
 - In addition to coordination with signal controllers to ultimately reduce or eliminate conflicts in the data, the role of continuous monitoring of the intersection (and cause the CI to transition to Suspended State) is included in the *SCMS Manager Intersection Validation Misbehavior Management* report. Accomplishing this is a goal of Stage 2.
 - Establishing an industry exchange of multiple signal controller manufacturers that support IOOs at all levels is key to national safety advantages that will result from validated CIs on city, county, and state operated roadways.
- The exploration of MAP message validation identified at least two additional tools for MAP validation (e.g., new and existing LiDAR road scans and the use of CIMMS). MAP messages are critical to achieving the safety benefits of CIs; it is recognized that financial and technical resources to dedicate to MAP messages will vary for IOOs. The number of intersections made safer as CIs will increase by establishing multiple tools for MAP validation to support different budgets.
- At the onset of this project, it was recognized that a Stage 2 At-Scale Implementation would be needed to expand the UDOT reference implementation corridor to additional corridors. The Stage 2 effort will serve as an intermediary next step to help achieve a critical number of validated CIs before production vehicles with CV safety applications are released. The Stage 2 At-Scale Implementation objectives are better understood now, and the emphasis will be on advancing the collaboration with multiple signal controllers and expanded introduction of MAP validation to explore the industry support, relative accuracy, and costs for LiDAR road scan approaches.

Incentivize Private-Sector Investments or Partnerships

- The established collaboration between IOOs, OEMs, and SCMS Manager have created a mechanism for the quick resolution of challenges and barriers that occur between prototype and “at-scale” and have positively contributed to national deployment of OEM safety applications and IOO CIs.

Increase Resiliency

- The industry is expected to benefit from demonstrated integration of a transportation cybersecurity system ‘via secure over-the-air communication of data between infrastructure and vehicles owned and operated by different entities.
- The industry is expected to benefit from CIs being more consistent and interoperable based on the use of nationally available and recognized validation tools and processes.

4. Anticipated Costs and Benefits of At-Scale Implementation

This section describes the anticipated impacts and costs of at-scale implementation, as well as baseline data and the methods to estimate these impacts and costs for at-scale implementation.

4.1 Anticipated Impacts of At-Scale Implementation in the Statutory Areas

The areas identified in statutory language in the IIJA (Public Law 117-58 Sec 25005) that are anticipated to be impacted by at-scale implementation are described below.

Improve Safety and Improve Reliability

- IOOs throughout the US may benefit by modeling their CIs off the UDOT reference implementation corridor that was validated using the validation profile developed as part of this proof-of-concept in order to reduce deployment costs while achieving validated CIs.
- The test tools developed in this effort were made available to validate CIs nationally. This may help advance “at-scale” deployment quicker and encourage OEMs to hasten the use of RLVW and other safety applications in production vehicles.
- The processes developed by this effort reduced OEM concerns about CI data quality, setting a stage for having RLVW and other safety applications in production vehicles, which will lead to reductions in red-light running related crashes.
- Outreach to other IOOs made them aware of this effort, including the process for validating CIs and available testing tools, to facilitate quicker deployment of fully validated CIs.
- Test tools developed by this effort will help advance to “at-scale” deployment quicker and will encourage OEMs to hasten the use of RLVW and other safety applications in production vehicles.

Incentivize Private-Sector Investments or Partnerships

- Reduced OEM costs of testing or demonstrating safety applications by having access to or using the UDOT reference corridor.
- The process developed by this effort through SCMS Manager collaboration with OEMs and UDOT reduced OEM concerns about CI data quality that set a stage for having RLVW and other safety applications in production vehicles, which will lead to reductions in red-light running related crashes.
- The established collaboration between IOOs, OEMs, and SCMS Manager have created a mechanism for the quick resolution of challenges and barriers that occur between prototype and “at-scale” will have positively contributed to national deployment of OEM safety applications and IOO CIs.

Increase Resiliency

- The industry benefits from the demonstrated integration of a transportation cybersecurity system via secure over-the-air communication of data between infrastructure and vehicles owned and operated by different entities.
- Interoperability will enhance resiliency of CIs that follow a consistent validation process using nationally available and recognized validation tools.

4.2 Anticipated Costs of At-Scale Implementation

An overarching objective of this proof-of-concept was to understand what is needed (and how much it can be expected to cost) to accomplish fully validated CIs and to make that process reasonable and manageable for individual IOOs. The costs of this proof-of-concept effort were \$1.8M, however this included significant resource allocation for the development of testing tools and procedures for CI validation. Specific costs for testing CIs in Utah were tracked as they occurred in order to anticipate costs of at-scale implementation for validating CIs per intersection, including the equipment and labor hours and

procurement costs. Engagement with other IOOs via the CV PFS and their testing/sampling of the tools and processes will allow for more perspectives and better estimates of IOO time and costs to implement “at-scale” as part of the Stage 2 effort. In this effort, estimated costs to validate CIs were:

- \$3000 per CI for LiDAR data to validate the MAP message.
- \$350-\$450 per CI to collect and analyze data per test. (Note that additional data collection and analysis may be needed if the results do not validate the CI.)
- \$5000-\$5800 per TSCLT (i.e., data collection tool).

At this time, a key cost driver relates to the validation profile determined by SCMS Manager, understanding that the full suite of requirements presented in *CTI 4501 version 2* is not feasible to examine for every CI. That is, there was a recognition that trust in the CI implementation could be established based on testing a subset of requirements and confirming the accuracy of how that subset was implemented. Additional key cost drivers include:

- IOO staff time to prepare CIs for testing and validation. Even after deployment, significant time may be needed at a CI to troubleshoot identified issues both before and as a result of testing.
- Validation tools and data collection, with specific considerations regarding additional training needed, and how user friendly and time consuming the processes are. As one example, a comprehensive understanding of costs is not available for all data collection alternatives for executing the developed MAP validation approach, as it may conceivably be done via a new LiDAR road scan process, using existing LiDAR road scan data, a survey, using the CIMMS monitoring tool, or by some other means.
- Other party costs to operate and maintain a fully validated CI (e.g., SCMS provider).

Moving forward, as additional CIs are validated there is a potential for costs to go down over time given the increased IOO staff familiarity and experiences with validation processes and tools, availability of improved hardware and software products from vendors and signal control manufacturers, development of more streamlined testing tools, and availability of SCMS providers equipped to perform and support validation.

Sources of uncertainty at this time relate to the timeline for releasing updated available hardware and software (i.e., from signal controller manufacturers) required to fully validate a CI, as well as access to and maintenance of testing and validation tools, specific data collection tools and approaches that will be ultimately required for validating CIs, and the development and availability of streamlined processes and tools that may reduce the costs to test and validate CIs in the future.

4.3 Methods to Estimate Anticipated Benefits and Costs Associated with At-Scale Implementation

The safety risks to pedestrians and drivers of all vehicles when red-light running events occur are recognized industry wide. RLVW applications have long been identified as an approach to reduce the occurrence of red light running. Additionally, the developed testing tools and validation processes provide a foundation for expanding them to support testing activities needed to validate CIs for the use of other applications. Since the focus of this project and evaluation was on assessing the extent to which the tools and processes developed were accepted by the industry, the evaluation did not attempt to estimate the quantitative safety benefits (i.e., no estimate of the number of crashes to be prevented were developed). Rather, the benefits were assessed by the extent to which OEMs and IOOs have increased knowledge about and trust in the processes and tools developed. As substantial gains were achieved in these areas, there are inferred benefits in coming years when RLVW and other safety applications are deployed and supported by IOO operated CIs.

The costs of at-scale implementation of the tools and processes were estimated by the time and effort expended by Utah in utilizing the resources developed to validate their CIs. Specifically, the estimated time to conduct specific testing activities at a CI are:

- Configuring the TSCLT (i.e., the data collection tool for testing) to match a given traffic signal cabinet: 15 minutes.

- Install TSCLT in cabinet, including both the physical install and testing to ensure messages are being received: 30 minutes.
- TSP and preemption during testing, including watching the traffic signal controller to ensure a timing plan change takes place, then priority on two approaches and preemption on two approaches with a delay between each priority or preemption for the traffic signal to return to coordination for two cycles: about 45 minutes.
- Remove TSCLT from cabinet: 15 minutes.

In total, this results in about 1 hour and 45 minutes of staff time to conduct validation testing at each CI. From this, a reasonable estimated range for the cost to test each CI a single time is about \$350-\$450. However, many variables will affect the ultimate total cost to validate a CI that will likely cause this estimate to rise. These variables include:

- Staff experience with testing tools and related activities to conduct testing in a timely manner. (Note that these processes are described in the *2024 Traffic Signal Cabinet Logging Tool Quick Reference Guide*.)
- Staff experience in terms of years of experience and seniority (i.e., senior staff versus junior staff).
- Driving time from the office site to a CI and between each CI being tested.
- Potentially significant time to conduct preliminary testing activities to ensure the CI meets requirements prior to conducting formal validation testing.
- Additional time to make adjustments to the CI and repeat formal validation testing each time the CI does not pass the validation test.

Additionally, LiDAR data was procured at a cost of \$3000 per CI to validate the MAP message; in this effort, LiDAR data was procured for 11 CIs at a cost of \$33,000.

Finally, the equipment cost for each TSCLT logging tool built in this effort was \$3800, plus 6-8 hours of staff time to assemble and test the tool for an additional \$1200-\$2000; this yields an estimated cost of \$5000-\$5800 per TSCLT. The OBU represented the most significant equipment cost at \$3618, while other equipment components for the TSCLT included a protective case, a 5-port managed switch, 12 Volts Direct Current power supply, power inlet and switch, power cords, and ethernet cables. As above, the amount of time required to assemble and test the tool may vary based on staff experience.

Engagement with other IOOs via the CV PFS and their testing/sampling of the tools and processes with CAMP through the UDOT SMART Grant Stage 2 activities in other locations will allow for more perspectives and better estimates of IOO time and costs to implement “at-scale”.

4.4 Baseline Data for At-Scale Implementation

Baseline data collected during this Stage 1 effort for at-scale implementation was:

- Baseline status of CIs nationwide – No CI deployments were proven to meet the full spectrum of requirements outlined in CTI 4501 version 02, and no CI deployments were recognized by OEMs or SCMS Manager as fully validated. Testing activities conducted at CIs in Utah identified minor issues that were not completely addressed by the end of the Stage 1 effort to be considered fully validated by OEMs or SCMS Manager. Note there is an understanding by OEMs and SCMS Manager that a CI may be considered fully validated in the near term until some outstanding issues preventing full compliance with CTI 4501 version 02 are addressed by traffic signal controller manufacturers.
- Baseline status of UDOT Connected Corridor(s) including gaps – Based on testing and validation activities conducted as a part of the SMART Stage 1 effort, gaps were identified to understand remaining needs to achieve validated CIs meeting the validation profile, which testing tools and procedures are able to detect and confirm.

- Baseline status of knowledge of CI validation processes – Testing tools and procedures are available to validate CIs against the validation profile. Additional experience is required to better understand the costs and potential efficiencies of validating CIs at scale.
- Baseline status of OEM concerns the quality and consistency of CI data – To date, OEMs are gaining trust in the data broadcast by CIs that are able to be validated against the validation profile based on the testing tools and procedures developed by this effort, which has helped to reduce this barrier towards implementation of RLVW applications.

5. Challenges, Best Practices, and Recommendations for Future Deployers

This section describes some considerations, lessons learned, and insights that arose over the course of this SMART Stage 1 effort that may assist future deployers with fully validating CIs in their jurisdictions. Solutions have not yet been identified for all challenges or unknowns, some of which remain unknown due to the limited nature of this Stage 1 effort. Future efforts, including a Stage 2 effort, will help practitioners better understand the costs, operations and maintenance considerations, the ability to streamline developed processes, and level of effort and needs for expanding workforce capability.

- **Procurement and budget.**

- *Challenge:* If LiDAR services or datasets are selected for MAP validation, the cost and timing to procure and schedule these services may be a challenge for agencies. For instance, while these services are already used by agencies for asset management purposes, adjusting contracts or specifications to gather the very specific data that are needed to validate the MAP message (particularly for intersecting roadways that are within a different jurisdiction beyond what is typically procured by the agency) may add extra time and cost.
- *Challenge:* The support services required to conduct preliminary testing and prepare a CI for validation is an additional budget consideration that could vary based on workforce capability.

- **Technology sustainability / integration with incumbent systems.**

- *Challenge:* The preparations to achieve a fully validated CI may encounter several challenges as it relates to incumbent systems and processes. Updates may be required if signal controllers used in the field are not able to provide accurate and complete SPaT data needed to support a fully validated CI, for example.
- *Challenge:* Issues identified at CIs that have already been tested will need to be addressed and, depending on the mechanism for addressing them, could in some ways be a bigger challenge than untested CIs (e.g., given a heightened urgency to maintain existing functionalities in an accurate, safe, and secure manner).
- *Recommendation:* The *SCMS Manager Intersection Validation Misbehavior Management* report considers the impact of misbehavior information provided by the CIMMS process.
- *Challenge:* Work is still underway to understand the need for RTCM validation. More broadly, the specific need and value of RTCM is not yet fully understood for various circumstances, specifically where it may be needed via what sources and in what locations. The CTI 4501 Requirements regarding RTCM are not as specific as other requirements regarding performance and part of the research of this project is to explore whether additional clarification about RTCM performance can be captured.
- *Recommendation:* Agencies may consider whether it is possible to validate a MAP message with LiDAR services as part of the same process that an agency already uses for asset management purposes.
- *Challenge:* The CTI Connected Intersections Implementation Guide 4501 v01.01 provides the RTCM message user needs, requirements, and design. An updated version of CTI 4501 expected to be released in 2025 will contain just the user needs while the requirements, design, validation test cases and procedures will be included in the SAE J3258 report. While not in the scope of the Utah SMART Grant project, the project team decided to attempt to approach this as an initial pilot site for validating that broadcast RTCM corrections messages were consistent with the updated CTI 4501 requirements. This included not only providing CIs that supported the requirements but also supporting the hardware and software validation tool efforts and executing the documented CTI 4501 validation test procedures. In advance of a final validation test tool, a prototype test tool was developed to evaluate corrections performance for a variety of Global Navigation Satellite

Systems (GNSS) configurations and test environments including some in the Salt Lake City area. The results of these efforts will be documented in SAE J3258. A challenge in completing these activities was that, as of the writing of this report, the requirements and design for the RTCM corrections messages were not complete, thus the validation test tool and testing activities described above were not able to be performed during stage one. The SAE J3258 requirements and corresponding validation test cases and procedures are anticipated to be completed within the second quarter of 2025. The primary changes will address which GNSSs, messages, and frequencies are to be supported as well as how this information is incorporated into the SAE J2735 message.

- *Recommendation:* Needed RTCM test tool and validation activities (which are proposed to be undertaken in stage two SMART Grant activities in Utah), include:
 - Upgrading the CI to support the SAE J3258 requirements.
 - Developing the validation test tool hardware including adding a mobile ground truth system to the prototype test tool to support performing mobile positioning accuracy analysis.
 - Developing the validation test tool analysis software.
 - Running the validation test procedures as defined in SAE J3258 and generating validation reports.
 - Provide feedback on gaps, issues, and / or improvements for SAE J3258.
 - Consider adding real-time monitoring to detect anomalies in the provided RTCM corrections data.
 - Packaging the hardware validation tool in a format that can be easily shared with other pilot sites for performing RTCM validation at their CI.
- **Data governance.**
 - *Challenge:* CIMMS data storage needs currently can incur relatively high costs for a single CI that is not sustainable for scalability in the long term. Determining what and how much data for testing is “good enough” remains a challenge that has not yet been addressed.
- **Cybersecurity.**
 - *Challenge:* Threats to critical infrastructure are abundant, however a true understanding of the different types of potential risks associated with fully validated CIs remains elusive. The proposed security requirements in *CTI 4501 version 02* do not appear to be testable or realistically achievable by IOOs in the near term, and so it will be necessary to identify an acceptable approach to security.
 - *Recommendation:* The ISS *CTI 4501 Security Policy Profile* resource developed by this effort provides a recommended solution for applying the CTI 4501 v02 requirements to securely deploy CIs.
- **Workforce capability.**
 - *Challenge:* The processes needed to prepare and conduct CI testing and validation, as well as address the variety of technical issues that may arise in the meantime, are not well understood by many agencies.
 - *Recommendation:* Training and knowledge transfer will be needed to prepare others in the workforce for at-scale deployment; UDOT is prepared to support this through engagement of neighboring state and local agencies.
- **Partnerships.**
 - *Best practice:* This effort demonstrated a successful collaboration between IOOs, OEMs, and SCMS Manager that is a model for moving forward as testing tools and procedures are further refined and implemented by additional deployers.
 - *Recommendation:* Other IOOs intending to fully validate CIs is possible and encouraged as part of the partnerships created in this effort.

6. Deployment Readiness

The SMART Stage 1 effort has certainly advanced the state of the practice for achieving fully validated CIs, and this section summarizes the readiness of this effort for at-scale implementation. More agency experiences are needed to better understand the scalability and long-term impacts of operating and maintaining validated CIs, which is also described below.

6.1 Project Readiness for At-Scale Implementation

The proof-of-concept successfully demonstrated that further expansion to at-scale implementation is feasible, as described below.

Requirements for Successful At-Scale Implementation

Feedback from CAMP's involvement in this initiative has indicated that remaining barriers to OEMs including V2X technologies in production vehicles are: lack of trust in CI data and the number of validated CIs deployed (note that the November 2024 release of the Second Report and Order from FCC removes a third previously identified barrier). There are several things this effort has influenced:

- Completion of the CI validation tools and approaches for both SPaT and MAP validation.
- Finalizing SCMS Manager Processes and Policies for validating CIs.
- Encouraging agency deployment and validation of CIs by introducing the process and tools to CV PFS member agencies, which expressed interest in using the testing tools and procedures developed as part of this effort.

Note that there is an understanding that developed tools, procedures, and overall data collection and analysis process, which are now available to other IOOs and described in Appendix B, are expected to be refined and enhanced in the future based on experiences and lessons learned, especially as additional state and local agencies expand their use of these tools and procedures.

Strategies or Demonstrated Progress

The progress for achieving goals for this effort include:

- The testing tools and software worked and were successful at identifying where *CTI 4501* requirements were not met. The CIs identified for this effort were validated using the developed tools and validation processes.
- Feedback from OEMs in CAMP and SCMS Manager indicated that stated project goals and outcomes were achieved.
- Project activities achieved desired outcomes per the performance measures identified in the Evaluation Plan. While challenges arose, the project team identified alternatives that still accomplished the overall trust in the CI data, as needed by OEMs, CAMP, and SCMS Manager.

Key Obstacles to Scaling this Project

Several issues arose over the course of this effort related to technology sustainability, workforce capability, and procurement and budget, and could impact the feasibility of fully validating CIs:

- CIMMS data storage needs remain uncertain and currently incur costs that are not feasible for at-scale deployment. However, efforts are currently underway to streamline data processing that would reduce data storage requirements, and associated costs.
- Signal controller variations and issues may hinder at-scale deployment. The testing and validation tools developed as part of this effort identified previously unknown issues; while this is a sign that the tools work as intended, it also means that additional issues could be identified while testing

other signal controller types and configurations in Stage 2. Some of these issues require updates from the signal controller manufacturers themselves, and as such may not be quickly resolved to allow for validation of all CTI 4501 requirements.

- Costs are a potential obstacle for agencies to scale CI validation more broadly. For instance, if the developed test tools and validation processes are too complex for IOOs to achieve with the available workforce, there is a risk that agencies will not see the benefit of dedicating resources to validate CIs, particularly without OEM production vehicles that support V2X safety applications.
- Agency preparation for CI validation requires workforce capabilities that may exceed some agency resources. Specifically, UDOT has worked for years to deploy and test CIs, resulting in staff and contractor experiences with V2X equipment to support troubleshooting and resolving identified issues; while the barriers to testing and validating CIs are now lower as a result of this effort, a learning curve will still exist for agencies that have less deployment experience.

6.2 Gaps in Understanding Maintenance and Operating Requirements

Given the limited experiences nationally with CIs, and remaining unknowns about requirements for ongoing monitoring of a validated CI, a number of gaps remain in understanding the maintenance and operating requirements for a fully validated CI. These gaps include the following:

- Enabling technologies and software are still being developed, resulting in a limited understanding of long-term maintenance needs, and are yet to be operated or deployed at scale.
- The process for monitoring and ongoing validation requirements is likely to evolve, and the tools for monitoring and validation, such as CIMMS are still being refined and expanded to be more robust.
- There is limited to no data available to help IOOs understand the long-term costs of maintaining CIs and the associated supporting systems and processes.
- Unforeseen cybersecurity challenges exist, and the requirements for ensuring security at a fully validated CI have not yet been determined.

6.3 Assessment of At-Scale Implementation: Harnessing Benefits and Mitigating Negative Impacts

There are no identified negative impacts of new technologies associated with fully validated CIs on the availability of good-paying jobs with the choice to join a union.

7. Wrap Up

Overall, the solution that was developed and demonstrated as a part of the UDOT Stage 1 SMART Grant effort met expectations. The tests and procedures developed are sufficiently robust to validate CIs. One key finding was that the tools and preliminary testing identified previously unknown issues in the signal controllers that the project team continues to work to address with the signal control manufacturers but were not able to be resolved during the project period. A description of supporting resources for the tools and processes developed as a part of this effort are presented in Appendix B.

Given the consensus and confidence in the test tools and procedures for CI validation by OEMs and CAMP, as well as the experiences and input from UDOT and other IOOs, the proof-of-concept was successful in achieving its goals and objectives.

Any IOO considering plans to validate CIs should bear several things in mind:

- Some issues identified as part of this UDOT effort still require updates from signal controller manufacturers to be a fully validated CI. However, the testing tools and validation processes developed as part of this effort are available to validate CIs against a profile or subset of CI requirements as defined by SCMS Manager.
- CI technologies and monitoring tools, as well as the test tools and validation procedures developed as part of this effort, are all in the early stages of deployment. As such, continued evolution is expected to occur as other issues are identified; however, efficiencies are anticipated over time. For example, agency staff may be able to conduct testing activities faster given increased experience with tools and troubleshooting, and technology solutions may be streamlined to hasten data collection and analysis.
- While OEM production vehicles are not yet equipped with RLWV and other safety applications, IOO commitments to deploy and validate CIs and other V2X solutions are needed to encourage OEM commitments.

8. Terms and Acronyms

8.1 Terms

Connected Intersections (CIs) are signalized intersections with connected vehicle (CV) technology, specifically infrastructure-based vehicle-to-everything (V2X) devices that broadcast messages about the intersection status (i.e., Signal Phase and Timing (SPaT) message, MAP message containing intersection geometry information, and Radio Technical Commission for Maritime Services (RTCM) message for position correction information). For the purposes of this effort, V2X devices are broadcasting messages within the 5.9 GHz spectrum using roadside units for low-latency CV safety applications; however, other applications and V2X devices may also or only use network cellular communications.

Red-Light Violation Warning (RLVW) is a key connected vehicle (CV) safety application being prepared for early deployment in equipped vehicles, which provides an in-vehicle warning to drivers that they are about to enter an intersection during a red light.

Validation and **verification** are two related terms that for the purposes of Connected Intersections (CIs) are used interchangeably to describe the process (and supporting tools) that will enable OEMs to trust that CIs deployed by IOOs are broadcasting accurate, consistent, reliable, and secured messages that can support in-vehicle Red-Light Violation Warning (RLVW) and other CI related safety applications.

8.2 Acronyms

C-V2X	Cellular-vehicle-to-everything
CAMP	Crash Avoidance Metrics Partners, LLC
CI	Connected intersection
CIMMS	Connected Intersection Message Monitoring System
CTI	Connected Transportation Interoperability
CV	Connected vehicle
CV PFS	Connected Vehicle Pooled Fund Study
DOT	Department of Transportation
FCC	Federal Communications Commission
IIJA	Investment and Jobs Act
IOO	Infrastructure owner operator
ISS	Integrated Security Services
ITE	Institute of Transportation Engineers
LiDAR	Light Detection and Ranging
OEM	Original equipment manufacturer
RLVW	Red-Light Violation Warning
RSU	Roadside unit
RTCM	Radio Technical Commission for Maritime Services
SAE	Society of Automotive Engineers International
SCMS	Security Credential Management System
SMART	Strengthening Mobility and Revolutionizing Transportation
SPaT	Signal phase and timing
TSCLT	Traffic Signal Cabinet Logging Tool
UDOT	Utah Department of Transportation
USDOT	United States Department of Transportation
V2X	Vehicle-to-everything

Appendix A: Signal Phase and Timing Testing Error Summary Table

Introduction

To evaluate the accuracy, consistency, and reliability of SPaT transmitted by CIs, the Traffic Signal Cabinet Logging Tool (TSCLT) was developed to serve several critical purposes. Briefly, the TSCLT:

- Collects serial data from the signal cabinet load switches – These load switches control the signal head and serve as ground truth for the status of each signal indication (e.g., red, yellow, green, flashing yellow arrow, etc.). This data is called the Signal Phase Event Log (SPEL) and is patterned after the Indiana Traffic Signal Hi Resolution Data Logger Enumerations.
- Receives OTA V2X messages – The embedded OBU receives the J2735 messages transmitted by the RSU.
- Logs the TSCBM message produced by the controller – This helps troubleshoot any issues encountered with the data since the TSCBM is the upstream source of SPaT.
- Logs the immediate forward messages (IFM) sent by the ECLA to the RSU – This helps troubleshoot any issues with the data and enables individual packets to be monitored at this intermediate step.
- Uses GNSS to acquire UTC time – A timestamp is applied to each data packet so that a single time source is used for all messages. This eliminates the challenge of comparing timestamps produced by devices with different time sources.

The CAMP data analysis software currently only uses the SPEL and the OTA datasets. The additional data collected by the TSCLT are used to troubleshoot discovered problems, track individual data packets, assess device performance, and determine the source of errors or poor OTA performance.

The TSCLT and CAMP's data analysis software successfully identified when SPaT was accurate, consistent, and reliable, and when it was not. The CAMP software processes and analyzes SPaT for accuracy, latency, and periodicity, and produces summary reports that provide results and whether the requirements in CTI 4501 were met.

However, a simple pass/fail determination does not fully capture the frequency, nor the magnitude, with which a requirement was not met. The results presented help fill this knowledge gap and provide more granularity into the accuracy, consistency, and reliability of SPaT.

Metrics

This section describes what information is included in the result table and its significance.

- SIG # – A unique identifier for signalized intersections.
- Date – Date when the data was collected (yymmdd).
- RSU – Identifies the RSU vendor whose device was used during the test. Distinct differences were observed between the two RSU vendors that impacted CTI 4501 compliance.
- MSGs – Lists the J2735 messages transmitted during the test.
- SPaT Collection – Identifies the SPaT collection method (OTA or IFM). OTA means the over-the-air SPaT transmitted by the RSU and received by the TSCLT. IFM means the immediate forward messages sent by the ECLA to the RSU for broadcast
- Timestamp – Identifies what timestamp is evaluated.

- SPaT MSG – Timestamp found within the SPaT message itself (a combination of the MinuteOfTheYear and DSecond data elements).
 - TSCLT Rx – Timestamp when the OTA SPaT is received by the TSCLT.
 - IFM – Timestamp when the ECLA sends SPaT to the RSU for broadcast.
- n – The number of SPaT messages collected.
- Single Message SPaT Periodicity – These metrics assess the consistency of SPaT according to the designed single message periodicity of one message every 100 +/- 25 ms.
 - Min – Minimum observed single message periodicity.
 - Percentile 75 ms – Percent of SPaT with a periodicity ≤ 75 ms. This is the acceptable lower limit for all timestamps.
 - Percentile 125 ms – Percent of SPaT with a periodicity ≤ 125 ms. This is the acceptable upper limit for the SPaT MSG and IFM timestamps.
 - Percentile 175 ms – Percent of SPaT with a periodicity ≤ 175 ms. This is the acceptable upper limit for the TSCLT Rx timestamp because the RSU is afforded 50 ms to process (encode and apply security credentials) and broadcast each SPaT message.
 - Max – Maximum observed single message periodicity.
 - Single IPR – Single InterPercentile Range, which measures the percent of observations that fall within the acceptable upper and lower limits for periodicity.
- Cumulative SPaT Periodicity – These metrics assess the consistency of SPaT over a 10-consecutive message interval with the designed cumulative periodicity of 10 messages every 1.0 second +/- 25 ms.
 - Min – Minimum observed cumulative periodicity for 10 consecutive SPaT.
 - Percentile 975 ms – Percent of 10 consecutive SPaT with a cumulative periodicity ≤ 975 ms. This is the acceptable lower limit for all timestamps.
 - Percentile 1025 ms – Percent of 10 consecutive SPaT with a cumulative periodicity ≤ 1025 ms. This is the acceptable upper limit for the SPaT MSG and IFM timestamps.
 - Percentile 1075 ms – Percent of 10 consecutive SPaT with a cumulative periodicity ≤ 1075 ms. This is the acceptable upper limit for the TSCLT Rx timestamp because the RSU is afforded 50 ms to process (encode and apply security credentials) and broadcast each SPaT message.
 - Max – Maximum observed cumulative periodicity for 10 consecutive SPaT.
 - Cumulative IPR – Cumulative InterPercentile Range, which measures the percent of 10 consecutive SPaT message intervals that fall within the acceptable upper and lower limits for cumulative periodicity.
- SPaT Broadcast Latency – These metrics assess the reliability of SPaT to be broadcasted within 175 ms from the time the signal controller sets the corresponding signal indications. This is the calculated difference in the TSCLT-applied timestamps from the SPEL and the OTA datasets. For each phase, the first SPaT message indicating yellow is compared to the analogous yellow record in the SPEL. Since the emphasis of the RLVW application is thru movements, these results only include yellow phases for thru movements.
 - Min – Minimum observed latency

- Max – Maximum observed latency
- Minimum End Time Accuracy – These metrics assess the accuracy of the minEndTime value in SPaT for yellow phases. For each phase, the minEndTime value in the first SPaT message indicating yellow is compared to duration of yellow in the SPEL. The requirement is that the minEndTime accuracy be within 100 ms of the actual duration of yellow. Since the emphasis of the RLVW application is thru movements, these results only include minEndTime accuracy for thru movement yellow phases. It should be noted that minEndTime accuracy was worse for left turn phases.
 - Min – Minimum observed accuracy
 - Max – Maximum observed accuracy

Results

The following table shows results for the metrics previously described. While not comprehensive, data collected at these intersections on these days were specifically included to highlight a variety of issues and challenges that were observed. The table also includes some commentary that is helpful when interpreting the results and provides insights not contained in the results themselves.

SIG #	Date	RSU	MSGs	SPaT Collection	Timestamp	n	Single Message SPaT Periodicity					Cumulative SPaT Periodicity					NOTES	SPaT Broadcast Latency (< 175 ms)			Minimum End Time Accuracy (< 100 ms)			
							Percentiles				Single IPR	Percentiles				Cumulative IPR		Col R in TSC SPaT Msg_Yr_Perf_Analysis report		NOTES	Col S in TSC SPaT Msg_Yr_Perf_Analysis report		NOTES	
							Min (ms)	75 ms	125 ms	175 ms		Max (ms)	Min (ms)	975 ms	1025 ms			1075 ms	Max (ms)		min	max		min
7708	241008	Vendor A	MAP SPaT RTCM	OTA	SPaT MSG	35,802	0	0.02%	99.99%		18,399	99.97%	898	0.09%	99.94%	19,300	99.85%	66	133	- 1 instance with no OTA SPaT for 18.4 seconds. IFM log confirms ECLA sent all SPaT to RSU. - 1 instance with 1 skipped OTA SPaT. IFM log confirms ECLA sent all SPaT to RSU. - 3 instances where duplicate SPaT messages were transmitted by the RSU. IFM log confirms that ECLA sent the duplicated SPaTs to the RSU.	- For all transmitted SPaT, excellent broadcast latency in complete compliance is observed	0	3200	- During preemption events, minEndTime value from TSC is reliably incorrect. In all observations, the incorrect values are also in the TSCBM message. - 110 yellows for thru movements, 4 failed minEndTime accuracy (2 during preemption, 2 during regular operation) - 108 passing yellows reported a minEndTime within 11 ms of the actual duration
					TSCLT Rx	16	3.21%		99.99%	18,465	96.78%	873	0.42%		99.94%	19,366	99.53%							
	241009	Vendor B	MAP SPaT RTCM	OTA	SPaT MSG	35,994	55	0.01%	99.99%		171	99.99%	929	0.01%	99.99%	1,071	99.98%	43	62	- 3 messages are below the periodicity lower limit - 1 message exceeds the periodicity upper limit	- For all transmitted SPaT, excellent broadcast latency in complete compliance is observed	198	55392	- 114 yellows for thru movements, all failed minEndTime accuracy - All minEndTime errors were also incorrect in the TSCBM message.
					TSCLT Rx	48	0.01%		99.99%	185	99.99%	922	0.01%		99.99%	1,087	99.98%							
7710	241007	Vendor A	MAP SPaT RTCM	OTA	SPaT MSG	27,457	86	0.00%	81.89%		599	81.89%	995	0.00%	6.07%	1,801	6.07%	5894	526640	- In addition to the skipped SPaT, there is an approximate 8-second delay in SPaT transmission that occurs completely within the RSU. - During a preemption event, an extra yellow phase is recorded in SPaT, but it is not found in TSCBM, SPEL, or the actual ATSPM log. This results in erroneous calculations by the analysis software that attempts to pair non-matching yellow events and results in extremely large values (i.e., a maximum SPaT broadcast latency of 526640 ms). Excluding this error, the values range from 5894 to 6733.	- Extremely high and incorrect values for minEndTime are in the TSCBM message during preemption events, which mimics behavior observed at other intersections	158	56637	
					SPaT Rx	72	0.02%		76.76%	479	76.74%	940	0.06%		9.31%	1,707	9.25%							
				IFM	SPaT MSG	33,926	0	0.01%	100.00%		126	99.99%	899	0.03%	100.00%	1,015	99.97%							
					IFM	17	0.01%	100.00%		117	99.99%	892	0.03%	100.00%	1,016	99.97%								
7707	241010	Vendor B	MAP SPaT RTCM	OTA	SPaT MSG	44,993	0	0.06%	99.97%		537	99.90%	563	0.10%	99.88%	1,437	99.78%	28	55	- 2 instances where ECLA failed to generate SPaT for ~0.5 seconds. After this 0.5-second delay, 6 SPaT messages were sent in ~0.2 seconds. No SPaT messages were skipped. TSCBM log does not contain this delay and the TSC provided TSCBM data at the appropriate frequency (~every 150 ms). - 1 instance where ECLA sent a duplicate SPaT message to the RSU.	- For all transmitted SPaT, excellent broadcast latency in complete compliance is observed	125	35464	- Extremely high and incorrect values for minEndTime are in the TSCBM message during preemption events - Outside of preemption events, minEndTime accuracy is typically about 130 ms off of the actual yellow duration. However, deviations up to 3535 ms are observed.
					TSCLT Rx	4	0.06%		99.98%	544	99.89%	556	0.10%		99.90%	1,438	99.80%							

Appendix B: Supporting Resources Developed in this Effort

A series of documents were developed as part of this effort by the project team partners at the Crash Avoidance Metrics Partners Limited Liability Company (CAMP LLC) Consortium (i.e., CAMP), Security Credential Management System (SCMS) Manager, and INTEGRITY Security Services (ISS). While these documents are available on the [Utah Department of Transportation \(UDOT\) Transportation Technology webpage \(https://transportationtechnology.utah.gov/what-were-learning\)](https://transportationtechnology.utah.gov/what-were-learning), **readers are encouraged to directly check the webpages of these organizations for updated versions of these documents. That is, the documents developed as part of this effort, described below, and available on the UDOT webpage are version one resources that are expected to evolve in the near future as part of other efforts.** These resources are described below.

Assessment of SPaT Accuracy to Support RLVW Application (CAMP, December 2024). This report describes the development of data acquisition and analysis tool for verification of requirements specified in CTI 4501v01 and v02 for analysis of signal phase status and the corresponding timing information generated by the traffic signal controller infrastructure and broadcast of SPaT message by the RSU of a CI.

Assessing Node Point Accuracy in the SAE J2735 MAP Message (CAMP, August 2024). This paper describes the use of mobile LiDAR scan data to assess node point accuracy for three CIs located in southeast lower Michigan. Specifically, CTI 4501 establishes requirements for SAE J2735 MAP Message node point accuracy supporting in-vehicle RLVW applications. These requirements are specified in relation to pavement markings defining ingress and egress lane boundaries for mapped intersections. Commercial Mobile Mapping services typically use a combination of scanning LiDAR technology in conjunction with high accuracy positioning (GNSS / GPS) and multi-axis high-resolution photography to create 3D models of roadways which include the locations of lane markings, curbs, stop bars and crosswalks. This information can be used to verify that the node point accuracy requirements established in CTI 4501 are satisfied by the MAP message developed for a CI.

Validation Assessment & Analysis Software Toolset User Guide, Version 3.0 (CAMP, August 2025). This document serves as the user guide for a software toolset created for the CI Program developed under the Vehicle-to-Infrastructure 5 (V2I-5) Consortium of Ford, GM, and Nissan. This initiative was conducted to facilitate the deployment of CIs that provide Red Light Violation Warning (RLVW). This version of the guide was updated under the UDOT SMART Grant. The toolset contains six modules (software tools) that are designed to validate over-the-air transmission of SPaT and MAP messages to facilitate CI deployment for RLVW.

Traffic Signal Cabinet Logging Tool Quick Reference Guide (UDOT and The Narwhal Group, December 2024). The Traffic Signal Cabinet Logging Tool (TSCLT) is a device used to collect data from a CI, which can then be analyzed by various CAMP applications to determine whether those messages meet the CTI 4501 specification. This guide is meant to inform practitioners who will be deploying the TSCLT in (or near) a traffic signal cabinet for a CI.

SCMS Manager Intersection Validation and Certificate Issuance Policy (SCMS Manager, September 19, 2024). This document describes the role of the SCMS Manager in the implementation and enforcement of validated intersections. SCMS Providers which are authorized by the SCMS Manager to issue certificates to V2X stations must support the intersection validation procedures defined in this policy if they intend to issue credentials for validated intersections.

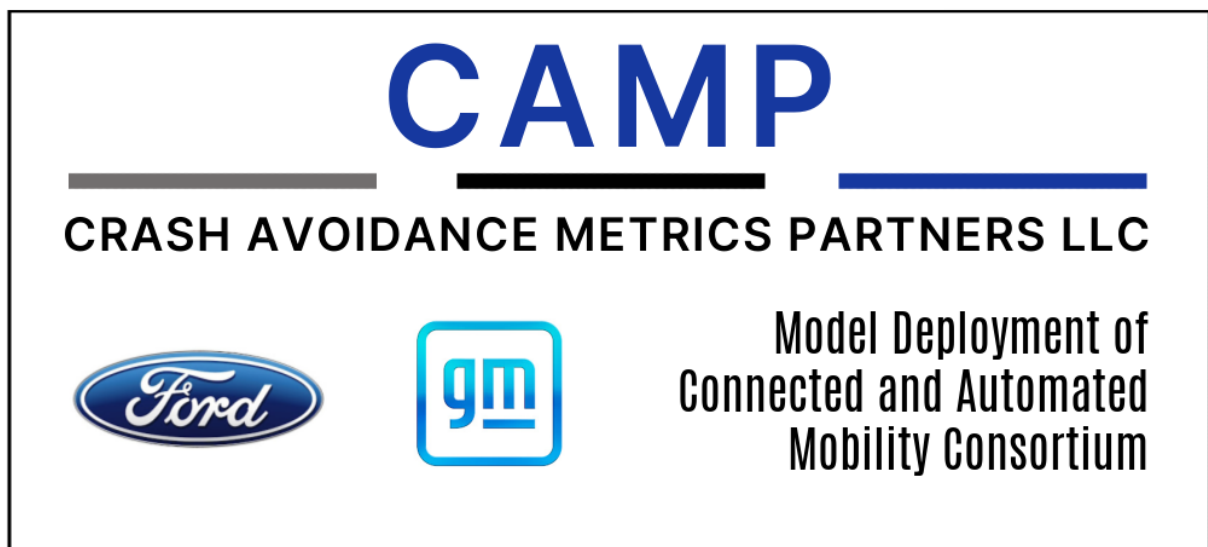
SCMS Manager Intersection Validation Misbehavior Management (SCMS Manager, December 23, 2024). This report considers the impact of misbehavior information provided by the Connected Intersections Message Monitoring System (CIMMS) process. This application collects data broadcast from a CI (in the form of SPaT and MAP data) along with BSM data from vehicles that drive through the intersection. It then performs analysis to compare the movement of vehicles (as reported in the BSM data) against the intersection status (as indicated in the SPaT and MAP data). Statistical data on misbehavior events is tracked against threshold values.

CI Test Results Report Format (ISS, May 31, 2024). This report outlines a recommended format for traffic organizations to use when providing cybersecurity test results for CIs to SCMS providers. This machine-readable format is crucial for maintaining accurate and up-to-date cybersecurity information throughout the lifecycle of the CI. By adopting this standardized format, SCMS providers can automate the certification process, ensuring continuous compliance and security monitoring, and enhancing the overall efficiency and effectiveness of the cybersecurity management for CIs.

CTI 4501 Security Policy Profile (ISS, August 20, 2024). This document specifically delineates requirements that either (a) apply exclusively to RSUs or (b) involve additional security controls necessitated by the installation of an RSU. By focusing on these specific scenarios, the document provides targeted guidance to ensure that RSUs are deployed and managed securely, minimizing potential vulnerabilities.

Utah SMART Grant – Enabling Trust and Deployment Through Verified Connected Intersections Project

Assessment of SPaT Accuracy to Support RLVT Application



Produced by Crash Avoidance Metrics Partners LLC in response to the United States Department of Transportation Project entitled “Enabling Trust and Deployment Through Verified Connected Intersections” under the SMART Grant program.

Report Documentation Page

Title and Subtitle Assessment of SPaT Accuracy to Support RLVW Application	Report Date December 2024
Author(s) Parikh, J.	
Performing Organization Name and Address Crash Avoidance Metrics Partners LLC on behalf of the Model Deployment of Connected and Automated Mobility (MDCAM) Consortium 27220 Haggerty Road, Suite D-1 Farmington Hills, MI 48331	Contract or Grant Utah SMART Grant – Enabling Trust and Deployment Through Verified Connected Intersections Project under the SMART Grant program.
Abstract <p>This report describes the development of data acquisition and analysis tool for verification of requirements specified in CTI 4501v01 and v02 for analysis of signal phase status and the corresponding timing information generated by the traffic signal controller infrastructure and broadcast of SPaT message by the RSU of a connected intersection.</p>	
Key Words Traffic, signal, controller, data, acquisition, tool, analysis, software, SPaT	

Table of Contents

Chapter 1.	Background	1
	Basis for SPaT Assessment	1
	Test Methodology	2
Chapter 2.	Traffic Controller Cabinet Data Acquisition Tool	3
	RS-485 Serial Bus Sniffer	4
	Supported Serial Cabinets	4
	Communication Bus Configuration	4
	Monitor and Capture Serial Data Frames	5
	Monitor and Capture SPaT Data	6
	TCCDAT Architecture	6
Chapter 3.	Field Test Setup	10
	Device: Traffic Signal Controller	10
	Device: RSU	11
Chapter 4.	CI Field Test Scenarios, Procedures and Time Plan	12
	Test Scenarios	12
	Test Time Plan	13
Chapter 5.	SPaT Analysis Software Toolset	15
	SPaT Message Broadcast Periodicity	16
	SPaT Accuracy and Latency Analysis	18
APPENDIX A.	Broadcast SPaT Message in JSON	20
APPENDIX B.	Processed SPaT Message Output	21
APPENDIX C.	SPaT Yellow Phase Performance Analysis	22
APPENDIX D.	SPaT Yellow Phase Performance Summary Report	23

Table of Tables

Table 1 - Example - Generated Signal Phase Event Log (SPEL) from Serial Data Frames 17

Table 2 - Converted Broadcast SPaT Message in PCAP to JSON 20

Table 3 - Partial List of Processed SPaT Messages in CSV 21

Table 4 - SPaT Message Structure and Required Data Elements Conformance Report..... 21

Table 5 - SPaT Yellow Phase Performance Analysis 22

Table 6 - SPaT Yellow Phase Performance Summary Report 23

Table of Figures

Figure 1 - Example Signal Cabinet Data Acquisition Tool.....3

Figure 2 - Traffic Controller Cabinet Serial Data Frame Sniffer4

Figure 3 - Data Process Flow in a Traffic Signal Field Cabinet.....5

Figure 4 - TCCDAT Interface Architecture to SPaT Data Acquisition Tool7

Figure 5 - Schematic of Information Flow to DAT.....8

Figure 6 - Steps in Processing and Analysis of SPaT Periodicity and MAP Message 15

Figure 7 - Inter Message Time Interval and Corresponding Distribution 16

Figure 8 - SPaT Analysis Process Flow..... 18

Figure 9 - Yellow Start Time Difference Between Controller and SPaT Message 19

Figure 10 - Yellow Duration Time Difference Between Controller and SPaT Message 19

List of Acronyms and Definitions

Acronym	Definition
AGP	Assured Green Period
ATC	Advanced Transportation Controller
ATSPM	Automated Traffic Signal Performance Measures
BIU	Bus Interface Unit
BSM	Basic Safety Message
C-V2X	Cellular Vehicle-to-Everything
CAMP	Crash Avoidance Metrics Partners LLC
CI	Connected Intersection
CIV	Connected Intersection Verification
CMU	Conflict Monitoring Unit
CSV	Comma separated Value
CTI	Connected Transportation Interoperability
DAT	Data Acquisition Tool
ECLA	External Control Local Application
GNSS	Global Navigation Satellite System
I2V	Infrastructure-to-Vehicle
IFM	Immediate Forward Mode
ITS	Intelligent Transportation System
JSON	JavaScript Objection Notation
MAP	Map data Message that Defines Roadway Geometry and Attributes
MDCAM	Model Deployment of Connected and Automated Mobility Consortium
MMU	Malfunction Monitoring Unit
MOY	Minute of the Year
MU	Mobile Unit

Acronym	Definition
NEMA	National Electrical Manufacturers Association
NTCIP	National Transportation Communications for ITS Protocol
OBU	On-board Unit
OTA	Over-The-Air
PCAP	Packet Capture
RLVW	Red Light Violation Warning
RSU	Roadside Unit
SAE	SAE International
SDLC	Synchronous Data Link Control
SIU	Serial Interface Unit
SPaT	Signal Phase and Timing
SPEL	Signal Phase Event Log
TCCDAT	Traffic Controller Cabinet Data Acquisition Tool
TSC	Traffic Signal Controller
TSCBM	Traffic Signal Controller Broadcast Message
TSP	Transit Signal Priority
UDOT	Utah Department of Transportation
UDP	User Datagram Protocol
UPER	Unaligned Packet Encoding Rule
USB	Universal Serial Bus
UTC	Universal Coordinated Time
V2I-5	Vehicle-to-Infrastructure Consortium 5
V2X	Vehicle to Everything

Chapter 1. Background

The deployed Vehicle-to-Everything (V2X) infrastructure for Connected Intersection (CI) requires meeting the minimum performance requirements set forth in the Connected Transportation Interoperability (CTI) Implementation Guide (CTI 4501v02) for guidance in support of in-vehicle Red Light Violation Warning (RLVW) application interoperability. Several criteria are established to assess and verify the CI performance.

- Accuracy – The CI infrastructure to broadcast accurate signal phase status and timing information
- Periodicity – The CI infrastructure to maintain consistent broadcast message periodicity
- Latency – The CI infrastructure to broadcast messages in timely manner

The report provides the necessary testing and validation methodology to verify the accuracy and utility of Signal Phase and Timing (SPaT) as per the SAE International (SAE) J2735 to support RLVW.

- As defined in SAE J2735 and established in CTI 4501v02, performance criteria for CI are required to meet the needs of the in-vehicle application addressing message accuracy, latency, stability and reliability of information flow.
- Test procedures and tools for data acquisition and validation are needed to determine how accurate the broadcast SPaT message data are relative to the actual signal controller actions.

This report includes:

- Required test data acquisition system and procedure to collect field data from the deployed connected intersection
- Various test scenarios to verify the real-world performance of the CI under test
- Analysis of the message structure, data format and required data elements as per J2735 and CTI 4501v02
- Analysis of the accuracy of broadcast the SPaT message relative to the actual signal controller actions that represents the ground truth for signal phase start time and the duration
- Analysis of the information processing latency of each link of the data flow across multiple devices for common CI configurations
- Analysis of stability and reliability of the information flow to connected vehicles

Basis for SPaT Assessment

The SAE J2735 SPaT message standard specifies the content and format of signal phase and timing information broadcast by a CI using Infrastructure-to-Vehicle (I2V) communications to support in-vehicle safety and mobility applications such as RLVW. The Connected Transportation Interoperability 4501v02 guide further specifies the desired SPaT data elements necessary to support RLVW. Basic RLVW application operates within the yellow phase time interval of a through movement which obviates the CTI 4501 requirements associated with Assured Green Period (AGP) for initial deployment.

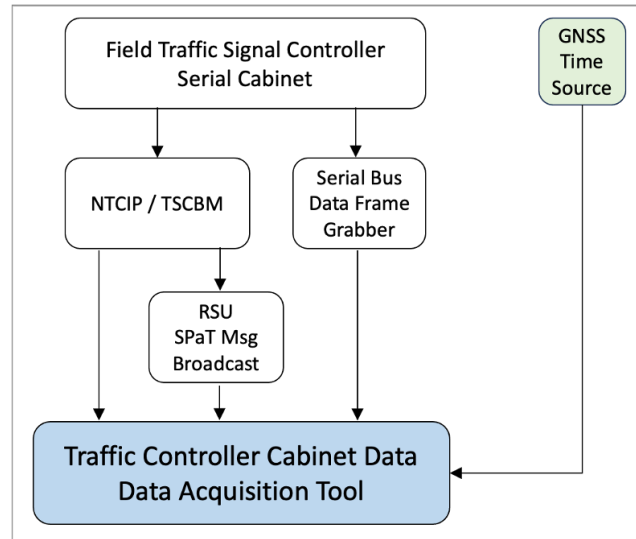
The purpose of this assessment tool and procedure is to verify that the duration of the yellow phase predicted by the Traffic Signal Controller (TSC) at the transition from green to yellow is accurate and that the broadcast of this information by the Roadside Unit (RSU) maintains a stable periodicity.

Test Methodology

To achieve V2X infrastructure application interoperability, a common test and validation methodology that includes field data acquisition system and SPaT data analysis tool is needed. Verification of the performance requirements specified in both the CTI 4501v01 and v02 guides requires analysis of signal phase status and the corresponding timing information generated by the TSC infrastructure and broadcast of SPaT message by the RSU.

Chapter 2. Traffic Controller Cabinet Data Acquisition Tool

Figure 1 shows an example of the Traffic Controller Cabinet Data Acquisition Tool (TCCDAT) or DAT to monitor and log signal phase and timing information generated by a connected intersection.



Source: Crash Avoidance Metrics Partners LLC (CAMP) Model Deployment of Connected and Automated Mobility (MDCAM) Consortium, 2024

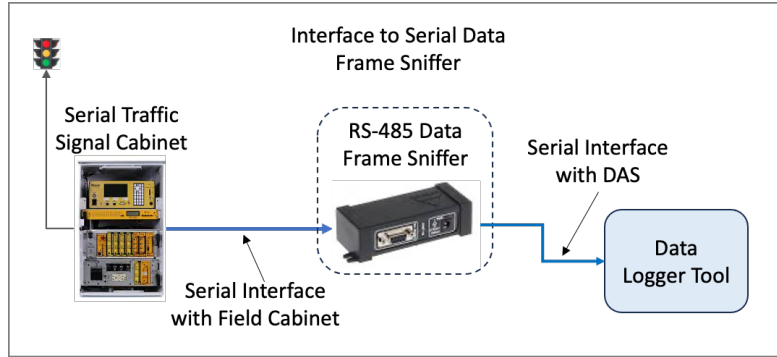
Figure 1 - Example Signal Cabinet Data Acquisition Tool

The DAT will monitor, capture and log the following data:

- Signal phase and timing information of the current and next signal phase status as commanded by the signal controller that actuate the signal lights
- Corresponding SPaT data generated by the traffic signal controller either in National Transportation Communications for Intelligent Transportation System (ITS) Protocol (NTCIP) standard or in Traffic Signal Controller Broadcast Message (TSCBM)
- Over-The-Air (OTA) Unaligned Packet Encoding Rule (UPER) encoded broadcast SPaT messages

For time-based data analysis, the internal clock of the data logger tool must be synchronized with the Global Navigation Satellite System (GNSS) time source to timestamp the data log with Universal Time Coordinated (UTC).

To monitor and capture appropriate data frames containing signal phase status, an RS-485 serial data frame sniffer is required to interface between the DAT and the communication bus in the cabinet is shown in Figure 2.



Source: Crash Avoidance Metrics Partners LLC (CAMP) Model Deployment of Connected and Automated Mobility (MDCAM) Consortium, 2024

Figure 2 - Traffic Controller Cabinet Serial Data Frame Sniffer

RS-485 Serial Bus Sniffer

The serial bus sniffer will interface with the Serial Interface Unit (SIU) and/or the Bus Interface Unit (BIU) as appropriate in the traffic signal cabinet and with the data logger over Universal Serial Bus (USB) for RS-485 serial bus communication protocol.

Supported Serial Cabinets

The following two types of serial cabinets are supported for serial bus interface that communicate controller commands and outputs to activate cabinet devices (e.g., load switches) and monitor inputs and communicate with other devices within the cabinet (e.g., Multifunction Monitoring Unit (MMU) / Conflict Monitoring Unit (CMU)).

- National Electrical Manufacturers Association (NEMA) cabinet (TS2 Type 1)
- An Advanced Transportation Controller (ATC) cabinet (ATC 5301v2)

The DAT through the RS-485 serial data frame sniffer will:

- Interface with appropriate SIU/BIU for Synchronous Data Link Control (SDLC) protocol to monitor and capture serial data frames
- Monitor and capture appropriate data frame that provides information to the SIU/BIU for signal indication outputs as on/off
- Monitor and capture appropriate data frame to determine the information sent to the SIU/BIU is being executed
- Monitor and capture appropriate response data frame for the on/off status of the assigned channels

Communication Bus Configuration

- The DAT should be configurable for the type of SIU and/or BIU present in the cabinet and appropriate communication port links with the interface unit(s)
- The DAT interface to the serial bus must not interfere with or interrupt the operation of the cabinet

- Notes:
 1. The serial bus data speeds are significantly different for the NEMA and the ATC serial cabinets. The DAT should be configurable to operate on both cabinet types.
 2. Some cabinets may include both the NEMA and ATC serial interfaces. The TCCDAT will support connection to both, however, not for simultaneous operation.
 3. The TCCDAT will be configurable for the types of BIU or SIU present and the device addresses for the serial interface unit. (e.g., with proper bus termination).

Monitor and Capture Serial Data Frames

- The DAT to determine output state change from on → off / off → on.
 - For each output, the DAT will log the transition type [on → off / off → on] and the time at which the transition occurred to determine flashing vs. steady state of signal indication.
 - The DAT will log the time of the transition within **TBD** milliseconds (i.e., the timestamp shall accurately indicate the time at which the transition commanded and the execution status to an accuracy of **TBD** milliseconds).
- The data process flow in a traffic signal field cabinet is illustrated in Figure 3.

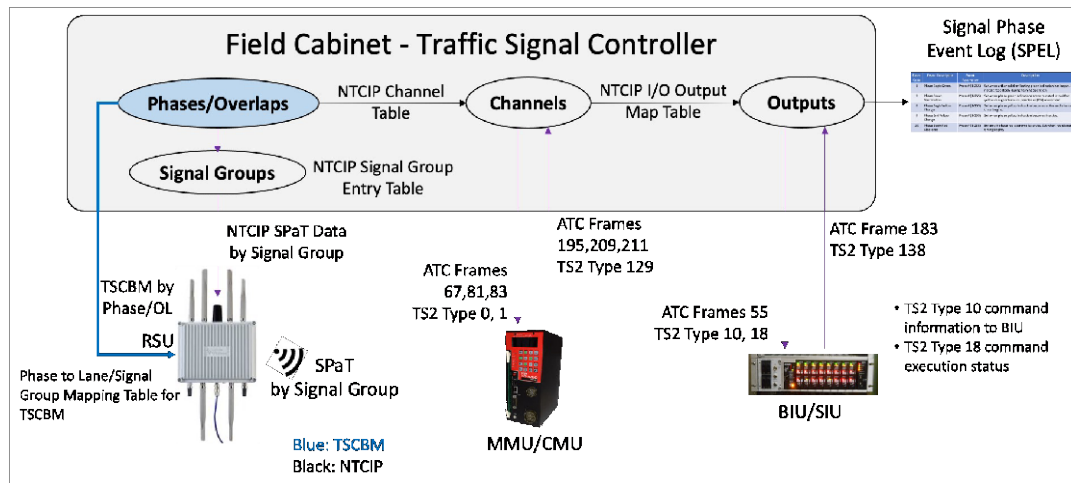


Figure 3 - Data Process Flow in a Traffic Signal Field Cabinet

- The DAT will examine the following data frames for:
 1. NEMA TS2 Cabinet
 - Frame Type 10 provides information to the BIU for outputs as on/off (+/-). This frame to be used to capture and examine the information sent to the BIU. Subsequently, frame Type 18 shall be captured and examined to determine that the information sent to the BIU is being executed. The data logging will capture and record the frames Type 10 and 18 and timestamp them. It is assumed that the BIU sends commands to subsequent devices within the cabinet to turn on/off commanded signal phase information to the signal indicator.

- Additionally, Type 138 response frame to be captured and examined from the BIU to determine the on/off status of assigned channels.
2. ATC Cabinet 5301v02 Cabinet
- Frame Type 55 sent to the SIU to be captured to examine the command to the module
 - Frame Type 183 from the SIU to be captured to verify that the commanded output is executed, and Ack is received (Ack only)

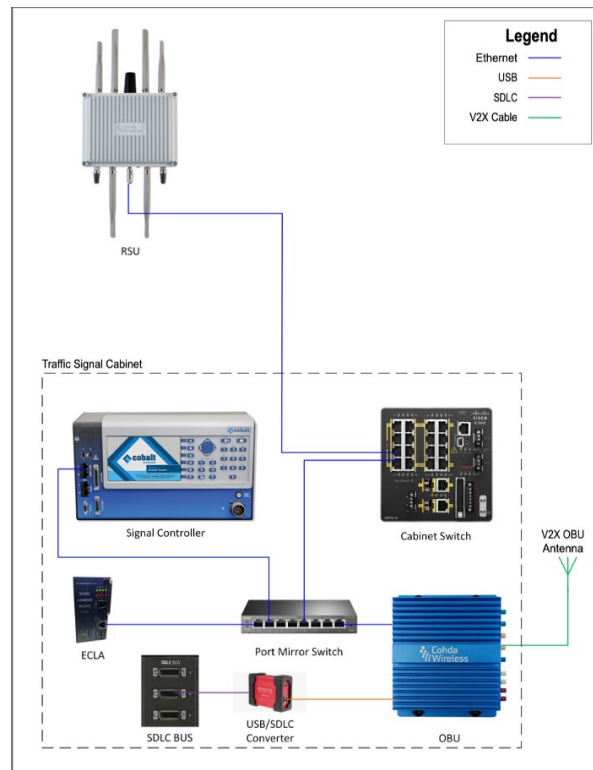
Monitor and Capture SPaT Data

It is required that DAT will simultaneously capture and log with timestamp the following streams of data.

- OTA SPaT message broadcast from the RSU
- Optionally, SPaT data generated by the signal controller in TSCBM (in future, can be replaced by NTCIP). Presently most deployed CI signal controllers generate signal phase status and timing data in TSCBM for generating SPaT message for broadcast in UPER encoded as per J2735. TSCBM data log may be useful for diagnosing where the issue lies in the TSC infrastructure.

TCCDAT Architecture

Figure 4 shows DAT interface and information flow architecture of a Cellular V2X (C-V2X) based receiver device (e.g., an On-Board Unit) or a similar Mobile Unit (MU) capable of receiving OTA V2X broadcast messages. The traffic controller cabinet DAT is a repurposed On-board Unit (OBU) with additional software used to perform data acquisition by capturing data from the traffic signal controller and from wireless and wired network sources. The DAT has a web interface that can be used to initiate data capture, log and download the data. The DAT is designed to collect data from various sources using a single time source in order to utilize Crash Avoidance Metrics Partners LLC's (CAMP) SPaT and MAP software analysis tools. These tools perform various checks and verifications to provide pass/fail test reports for compliance to CTI 4501v02.



Source: Crash Avoidance Metrics Partners LLC (CAMP) Model Deployment of Connected and Automated Mobility (MDCAM) Consortium, 2024

Figure 4 - TCCDAT Interface Architecture to SPaT Data Acquisition Tool

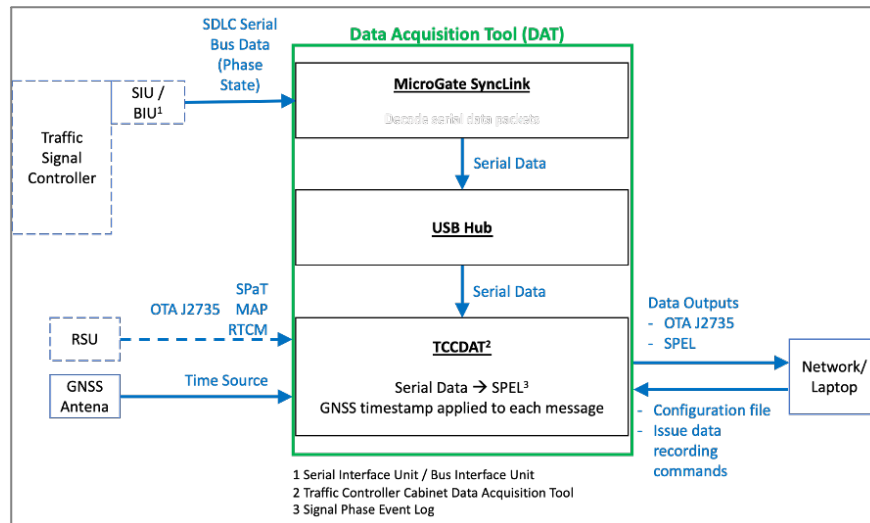
The TCCDAT supports:

1. A USB interface to sniff RS-485 serial bus data in the cabinet
2. An ethernet interface to communicate with an external device (e.g., External Control Local Application (ECLA) or an RSU) over ethernet User Datagram Protocol (UDP)
3. An ethernet network switch for managing data flow from multiple devices in the cabinet
4. A GNSS receiver for acquiring UTC time to synchronize internal clock of the DAT used to timestamp data log
5. A Cellular V2X antenna to receive OTA broadcast messages and a GNSS antenna to get UTC time (one source) to timestamp captured data
6. Data packet capture (PCAP) from the network (wired and wireless)
7. User interface for remote access and management of DAT to:
 - Setup test configuration including data file names
 - Initiate start/stop/pause/resume data logging process
 - Retrieve logged data files

For the UDOT Smart Grant Project, the DAT captures the following for SPaT verification.

1. TSC command frames from the SIU/BIU are converted into corresponding Signal Phase Event Log (SPEL) in Comma Separated Value (CSV) format. The log provides start and end times of signal phase events as commanded by the controller to determine the signal phase start time and its duration for comparing with the broadcast SPaT for accuracy.
2. Over-the-air data packets consisting of J2735 messages received by the DAT and transmitted from sources such as the RSU at the site, other RSUs in the proximity, and connected vehicles transmitting Basic Safety Message (BSM).
3. Data capture of SPaT in TSCBM as generated by traffic signal controller.
4. The message generated by an ECLA from TSCBM as a SPaT message for Immediate Forward Mode (IFM) to RSU to be broadcast.

To run the CAMP SPaT and MAP CTI 4501v01/v02 software compliance tool, only Steps 1 and 2 are required. However, if failures are reported in the compliance report, having the TSCBM and/or IFM data generated prior to the RSU for broadcast may be useful for diagnosing where and possibly why the failure(s) actually occurred. Figure 5 shows the schematic of information flow to DAT.



Source: Crash Avoidance Metrics Partners LLC (CAMP) Model Deployment of Connected and Automated Mobility (MDCAM) Consortium, 2024

Figure 5 - Schematic of Information Flow to DAT

DAT Setup in Traffic Controller Cabinet

In order to perform data capture for a given traffic signal cabinet, first a configuration of the cabinet must be created that includes which channels and overlaps are utilized by the traffic signal controller and what are the corresponding defined functions. This configuration is required for collecting serial bus data from the BIU and is used to interpret the serial commands from the traffic signal controller over the BIU for generating Signal Phase Event Log to compare with broad SPaT message for analysis.

In the Utah Department of Transportation (UDOT) CI architecture, an ECLA receives TSCBM messages and generates SPaT messages and sends the messages as IFM messages to the RSU to apply appropriate security credentials and broadcast. To capture TSCBM from the controller and IFM from the ECLA, an ethernet network switch capable of "port mirroring", i.e., the ability to duplicate network traffic from one or more ports on another port, is installed in the signal cabinet along with the DAT. The network switch is configured to mirror the ECLA's network port since it receives TSCBM messages from the traffic signal controller and transmits SPaT messages to the RSU. This additional network switch is connected to the cabinet's network switch, the traffic

signal controller and ECLA are moved to the new switch, and the DAT is connected to the mirror port. Also, the DAT must be given an IP address that is compatible with the network on which the ECLA and traffic signal controller are located.

When the data collection begins, a process is run in the DAT that initiates other processes for data collection from the various sources for a specified period of time. Each captured data record is timestamped. The initial process then waits until all the collection processes have completed and creates a report on the collection run in the directory where the various collected files were stored.

Chapter 3. Field Test Setup

Collecting data under all operating conditions would be a significant undertaking and falls outside the scope of this project. However, to provide reasonable assurance of CI verification, a variety of common scenarios, or test cases, have been identified that inherently disrupt and affect typical signal operations. Collecting data for each applicable use case enables the verification and validation of a CI and the data it broadcasts are accurate to satisfy the needs of in-vehicle RLVW application and requirements in CTI4501v02.

Device: Traffic Signal Controller

Test Case #	TSC-01	
Test Case	Traffic Signal Cabinet Serial Bus Data Frames	
Objective	Read SDLC serial bus data command frames that control voltage to the load switches.	
Requirements verified	CTI 4501v02 3.3.2.1.6 TSC Signal State Periodicity	A TSC infrastructure shall set the signal indications 10 times per second via the cabinet serial bus at 100 +/- 25 ms intervals where the duration of the 10 consecutive intervals is 1.0 seconds +/- 25 ms.
Brief Description	The load switches define the status of each signal face and corresponding signal indications. This is the raw source data that provides the command issued on the serial bus as the ground truth for the signal indications and what vehicle operators see.	
Test Procedure(s)	Connect RS-485 serial data frame sniffer of the DAT to the signal cabinet Serial Interface Unit/Bus Interface Unit as appropriate and via USB hub to the DAT.	

Test Case #	TSC-02	
Test Case	Serial Bus Data Frame Conversion	
Objective	Convert serial bus data to the SPEL	
Requirements verified	CTI 4501v02 3.3.2.1.7 TSC Signal Indication Phase State and SPaT Information Consistency	A TSC infrastructure shall send SPaT information messages to an RSU within 25 milliseconds of setting the corresponding signal indications.
Brief Description	Upon receiving the serial bus data, the DAT converts it to the SPEL, a data log patterned after the Indiana Traffic Signal Hi Resolution Data Logger Enumerations, or the controller even log.	
Data Outputs	Generate a SPEL file	
Test Procedure(s)	Sniff serial data frames and convert appropriate data frame to SPEL.	

Test Case #	TSC-03 (optional)	
Test Case	Traffic Signal Controller Broadcast Message (TSCBM) Data	
Objective	Verification of conversion of TSCBM data to SPaT message	

Requirements verified	CTI 4501v02 3.3.2.1.6 TSC Signal State Periodicity	A TSC infrastructure shall set the signal indications 10 times per second via the cabinet serial bus at 100 +/- 25 ms intervals where the duration of the 10 consecutive intervals is 1.0 seconds +/- 25 ms.
Brief Description	Controller generates intermediate SPaT data for generating UPER encoded SPaT message either by an ECLA or an RSU for OTA broadcast.	
Data Outputs	TSCBM data log file	
Test Procedure(s)	Connect to DAT through the port mirroring switch	

Device: RSU

Test Case #	RSU-01	
Test Case	J2735 SPaT Reception	
Objective	Receive and log OTA SPaT broadcast by RSU.	
Requirements verified	CTI 4501v02 3.3.3.1.5.4 SPaT Message - Broadcast Latency and Accuracy - Commanded	A connected intersection shall broadcast a SPaT message within 175 milliseconds from the time the TSC infrastructure sets the corresponding signal indications.
Brief Description	OTA SAE J2735 SPaT broadcast message receive and log for verification of message broadcast latency	
Data Outputs	Logged PCAP file with J2735 SPaT message	
Test Procedure(s)	DAT capture and log OTA broadcast messages from RSU in PCAP	

Chapter 4. CI Field Test Scenarios, Procedures and Time Plan

The following operational scenarios are identified that provide reasonable common real-world situations for SPaT verification under which typical signal operations are affected.

Test Scenarios

- OS - 1: Record Normal Signal Operations
 - Use the DAT to collect signal timing data when the traffic signal controller is operating under normal signal timing conditions.
- OS - 2: Record Timing Plan Transition
 - Use the DAT to collect signal timing data when the traffic signal controller transitions from one timing plan to another.
- OS - 3: Record Preemption – Early Green
 - Use the DAT to collect signal timing data when the traffic signal controller receives and serves early green preemption.
 - **Test Procedure**
 - Step 1: Confirm that the traffic signal controller is operating under normal signal timing conditions (i.e., it is not “in transition” or currently serving Transit Signal Priority (TSP) or preemption).
 - Step 2: Initiate a preemption call for a movement with a phase status of “red” such that a served preemption call will change the phase status to “green.”
 - Step 3: Confirm that preemption is served.
 - Step 4: Cancel the preemption call.
 - Step 5: Confirm that the traffic signal controller returns to normal operating conditions.
- OS - 4: Record Preemption – Green Extension
 - Use the DAT to collect signal timing data when the traffic signal controller receives and serves green extension preemption.
 - **Test Procedure**
 - Step 1: Confirm that the traffic signal controller is operating under normal signal timing conditions (i.e., it is not “in transition” or currently serving TSP or preemption).
 - Step 2: Initiate a preemption call for a movement with a phase status of “green” such that a served preemption call will maintain the phase status of “green” beyond the typical duration.
 - Step 3: Confirm that preemption is served.
 - Step 4: Cancel the preemption call.

- Step 5: Confirm that the traffic signal controller returns to normal operating conditions.
- OS - 5: Record TSP – Early Green
 - Use the DAT to collect signal timing data when the traffic signal controller receives and serves early green transit signal priority.
 - **Test Procedure**
 - Step 1: Confirm that the traffic signal controller is operating under normal signal timing conditions (i.e., it is not “in transition” or currently serving TSP or preemption).
 - Step 2: Initiate a TSP call for a movement with a phase status of “red” such that a served TSP call will change the phase status to “green.”
 - Step 3: Confirm that TSP is served.
 - Step 4: Cancel the TSP call.
 - Step 5: Confirm that the traffic signal controller returns to normal operating conditions.
- OS - 6: Record TSP – Green Extension
 - Use the DAT to collect signal timing data when the traffic signal controller receives and serves green extension transit signal priority.
 - **Test Procedure**
 - Step 1: Confirm that the traffic signal controller is operating under normal signal timing conditions (i.e., it is not “in transition” or currently serving TSP or preemption).
 - Step 2: Initiate a TSP call for a movement with a phase status of “green” such that a served TSP call will maintain the phase status of “green” beyond the typical duration.
 - Step 3: Confirm that TSP is served.
 - Step 4: Cancel the TSP call.
 - Step 5: Confirm that the traffic signal controller returns to normal operating conditions.
- OS – 7: Record Pedestrian Actuation.
 - Monitor pedestrian actuation throughout data collection period to determine if manual actuation is needed.

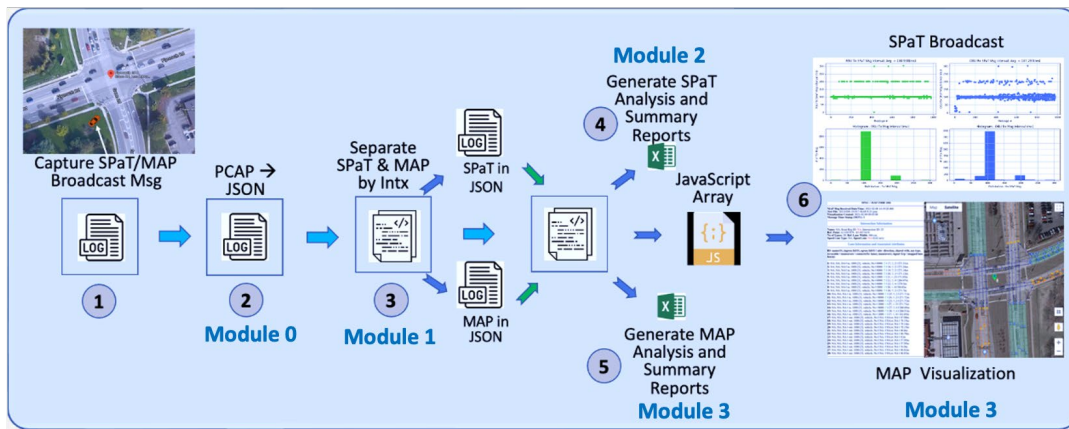
Test Time Plan

- Under most circumstances, data collection for the described operational scenarios, testing can be achieved as follows. For example:
 - Normal operation – 20 minutes
 - Time plan transition – 10 minutes
 - Signal preemption – 30 minutes
 - Early green
 - Green extension

- Transit signal priority – 30 minutes
 - Enable preemption Signal Request Message (SRM)
 - Early green
 - Green extension
- The test data collection time plan can be extended, if needed, to collect data under all applicable operational test scenarios. However, the time should not be reduced. Any additional time will result in longer data collection under “normal operation.”

Chapter 5. SPaT Analysis Software Toolset

A software toolset developed by CAMP under the Vehicle-to-Infrastructure 5 (V2I-5) Consortium (Ford, General Motors, Nissan) was further enhanced under the Connected Intersection Verification (CIV) Project to support deployment of CIs supporting RLVW. The toolset contains several modules (software tools) that allow the user to verify, analyze and assess over-the-air broadcast of SPaT and corresponding MAP messages. The toolset contains six major software modules. These modules process and analyze SPaT message broadcast accuracy, process latency and periodicity. Figure 6 shows the six steps involved in processing the SPaT and MAP logs contained in modules 0 through 3.



Source: Crash Avoidance Metrics Partners LLC (CAMP) Model Deployment of Connected and Automated Mobility (MDCAM) Consortium, 2024

Figure 6 - Steps in Processing and Analysis of SPaT Periodicity and MAP Message

- **Module 0: Message Conversion** – This module converts logged over-the-air broadcast messages (Packet Capture (PCAP)) in UPER to JavaScript Object Notation (JSON) for next step in processing. Appendix A shows an example of converted SPaT message in PCAP to JSON.
- **Module 1: Message Separation** – This module separates logged SPaT and MAP messages by intersection. The log may contain messages other than SPaT and MAP from multiple intersections due to the geographical proximity of CIs.
- **Module 2: SPaT Processing** – This module verifies the converted SPaT messages in JSON for conformity to SAE J2735 and CTI 4501v01 guidance for RLVW, generates the SPaT message log, and the conformance report in CSV (see Appendix B). Inter message time interval (periodicity) plots for visual verification are also generated in this module.
- **Module 3: MAP Processing** – This module assesses the converted MAP message to JSON for conformity to SAE J2735 and CTI 4501v01 guidance as well for RLVW, generates analysis reports, and builds appropriate data array for web browser-based MAP visualization and analysis.

SPaT Message Broadcast Periodicity

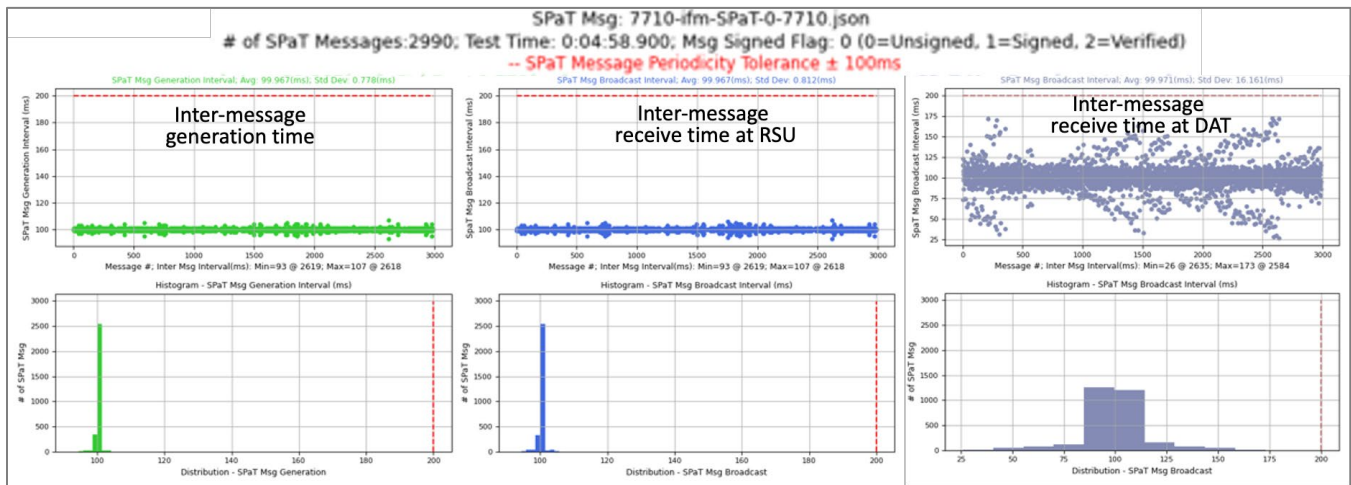
For RLVW application to perform as intended, a nominal 100 msec inter-message periodicity is highly desired. The periodicity of message generation from the controller data and message transmission by the RSU for inter message time interval is determined from the following timestamps in Module 2.

- 1) The SPaT message contains the time at which the SPaT message for broadcast is generated from the controller data typically in TSCBM from MinuteOfTheYear (MOY) and timeStamp data objects. The Module 2 verifies the periodicity (inter-message time) of message generation
- 2) Message received timestamp by the DAT.

As defined in CTI 4501, subsection 2.4.3.2.1 Time Source, a connected intersection needs to use the same time reference with sufficient precision and accuracy as OBUs/MUs. The DAT should also be designed to use the same time source as OBUs.

Figure 7 shows three plots of inter message time intervals.

- 1) Generated SPaT messages in green at ECLA.
- 2) Generated message transmitted to the RSU at port 1516 for IFM in blue for security credentials and message broadcast.
- 3) OTA message received by the DAT in light gray.



Source: Crash Avoidance Metrics Partners LLC (CAMP) Model Deployment of Connected and Automated Mobility (MDCAM) Consortium, 2024

Figure 7 - Inter Message Time Interval and Corresponding Distribution

As shown in plots, a stable periodicity of nominal time interval of 100 msec is maintained for SPaT message generation (green) and transmitted to the RSU (blue). However, the OTA broadcast message from the RSU (light gray) received by the DAT does not have stable periodicity as per the CTI 4501v02 Section 3.3.2.1.7 TSC Signal Indication Phase State and SPaT Information Consistency.

Signal Phase Event Log (SPEL)

To ensure required performance of the RLVW application, predicted time of start of yellow phase and duration for each signal in SPaT message must match with ground truth information generated by the traffic signal controller.

As described earlier, the TCCDAT is designed to monitor and capture the commanded signal light events from the serial bus. The captured data frames are converted to SPEL in CSV. An example of SPEL is shown in Table 1 for input to yellow phase analysis module.

Table 1 - Example - Generated Signal Phase Event Log (SPEL) from Serial Data Frames

Signal Id	UTC Timestamp	Event Code	Event Parameter
7710	2024-10-02T14:47:03.557+0000	7	4
7710	2024-10-02T14:47:03.557+0000	8	4
7710	2024-10-02T14:47:06.861+0000	9	4
7710	2024-10-02T14:47:06.861+0000	10	4
7710	2024-10-02T14:47:06.861+0000	12	4
7710	2024-10-02T14:47:09.356+0000	0	2
7710	2024-10-02T14:47:09.356+0000	1	2
7710	2024-10-02T14:47:09.356+0000	0	6
7710	2024-10-02T14:47:09.356+0000	1	6
7710	2024-10-02T14:47:46.656+0000	7	2
7710	2024-10-02T14:47:46.656+0000	8	2
7710	2024-10-02T14:47:51.156+0000	9	2
7710	2024-10-02T14:47:51.156+0000	10	2
7710	2024-10-02T14:47:51.156+0000	12	2
7710	2024-10-02T14:47:53.156+0000	0	1
7710	2024-10-02T14:47:53.156+0000	1	1
7710	2024-10-02T14:48:13.657+0000	7	1
7710	2024-10-02T14:48:13.657+0000	8	1

Where:

- Signal ID: Intersection ID
- UTC Timestamp: yyyy-mm-ddThh:mm:ss.sss±hh
 - Date: year-month-day
 - T: follows time
 - Time: hour:minute:second.milliseconds±hour offset
- Event Code: Signal Phase Event[†]
- Event Param: Signal group# (1–255)[†]
- File Format: Comma Separated Value

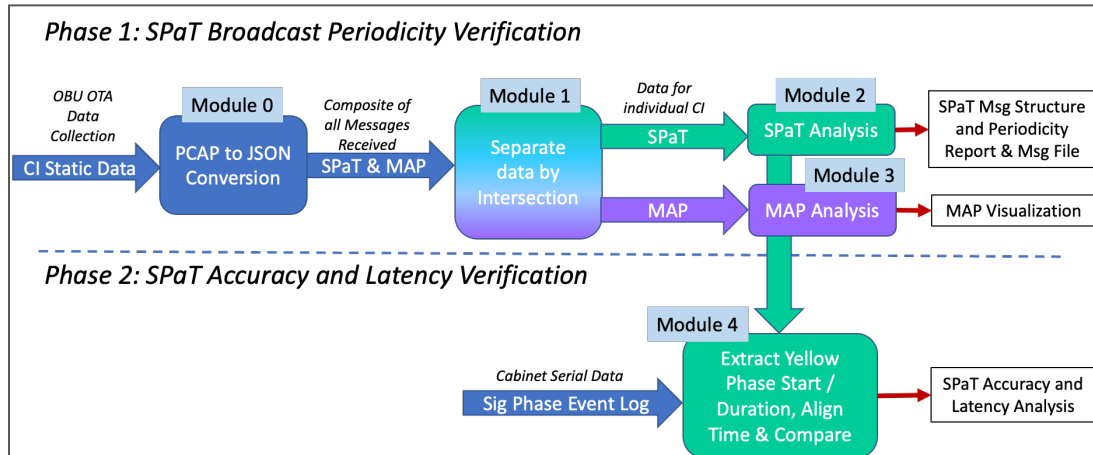
[†] For detail, see “Indiana Traffic Signal Hi Resolution Data Logger Enumerations”, August 2020 for detail at: <https://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1003&context=itrpdata>

In SPEL, the Signal ID indicates the intersection ID, the UTC Timestamp provides time in UTC, and the Event Code provides start and end of a signal phase. For yellow phase, value 8 indicates start and 9 indicates end for the signal phase given in the Event Parameter at the indicated timestamp.

In the current implementation of SPEL, the event code enumeration is adopted from the Automated Traffic Signal Performance Measures (ATSPM) as used in traffic data collection and performance measurement. However, it can be further enhanced with additional codes to log additional signal state events.

SPaT Accuracy and Latency Analysis

Figure 8 shows the progression and dependency of processing modules for SPaT analysis. Module 4 analyzes the start of yellow and its duration from the controller and in the broadcast message. The module is further enhanced in the current project to verify accuracy as generated by the traffic signal controller as the ground truth and how accurately it is reflected in broadcast SPaT message including end-to-end process latency.



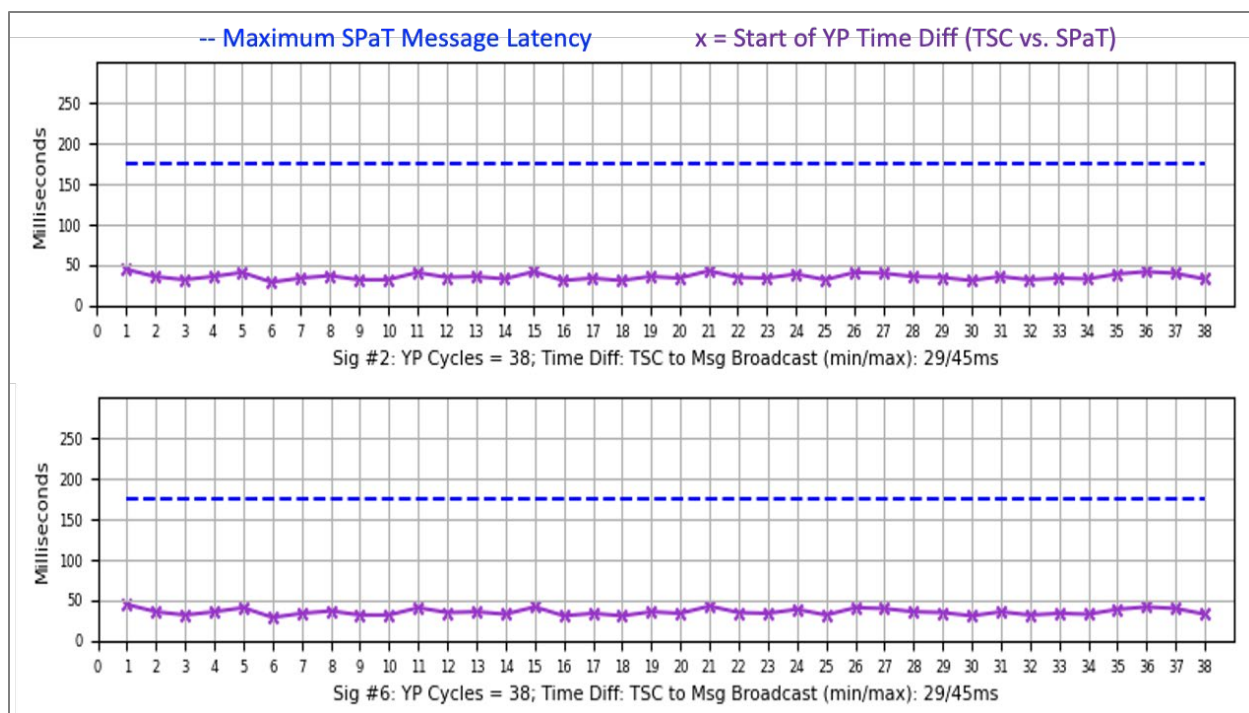
Source: Crash Avoidance Metrics Partners LLC (CAMP) Model Deployment of Connected and Automated Mobility (MDCAM) Consortium, 2024

Figure 8 - SPaT Analysis Process Flow

APPENDIX C shows example yellow phase performance summary and pass/fail report as per the requirements in CTI 4501v02.

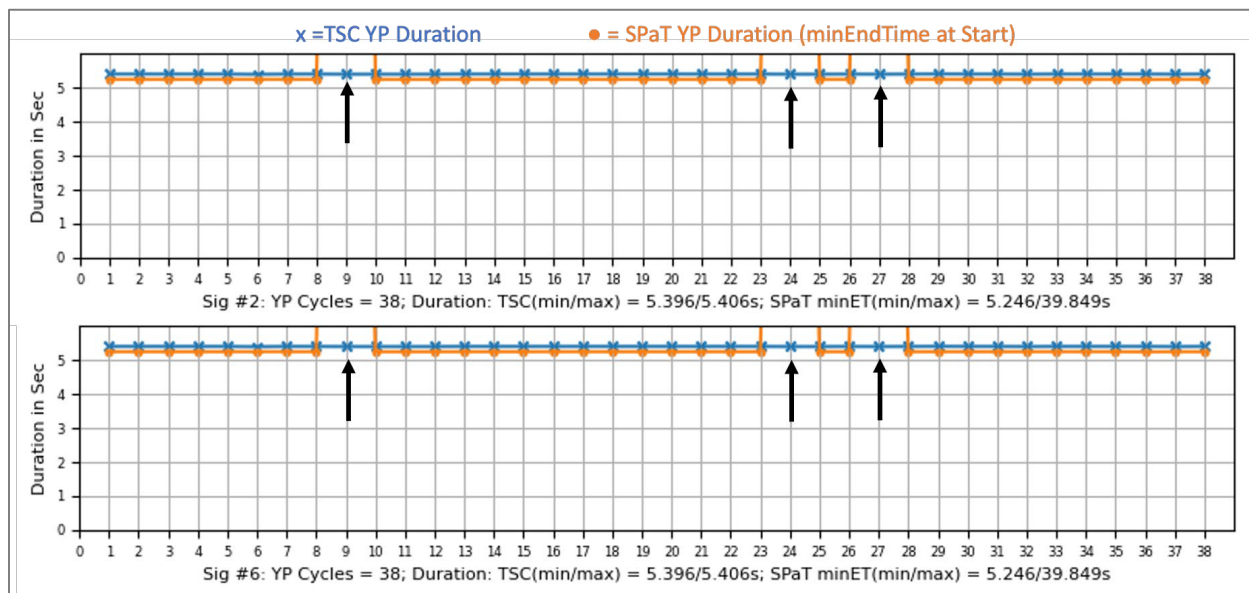
This module analyzes the start of yellow and its duration as indicated in the signal controller SPEL and in the corresponding SPaT message for data accuracy and latency. The results of test analysis for the test scenarios described in Chapter 4 for CI 7706 at State Route 224 and Sun Peak Drive at the UDOT is shown in Figure 9 and Figure 10. The plots show all occurrence of yellow cycles during the test for all eight signal groups. The plot in Figure 9, time difference of start of yellow between the controller and corresponding SPaT message is shown in purple. The difference varies between 29 msec and 45 msec, well within the required 85 msec (CTI 4501, Table 7 - Maximum SPaT Message Latency). The blue dash line indicates maximum required end-to-end transmission latency from the controller to the message broadcast.

The plot in Figure 10 shows yellow duration of 5.4 seconds in SPEL in blue, however in the SPaT message, shown in orange, it is 39.849 seconds at the time of signal preemption during the test as indicated by arrows for signal groups 2 and 6 in cycles 9, 24 and 27. Analysis of logged TSCBM data also indicates the same large value for yellow that is reflected in the SPaT message.



Source: Crash Avoidance Metrics Partners LLC (CAMP) Model Deployment of Connected and Automated Mobility (MDCAM) Consortium, 2024

Figure 9 - Yellow Start Time Difference Between Controller and SPaT Message



Source: Crash Avoidance Metrics Partners LLC (CAMP) Model Deployment of Connected and Automated Mobility (MDCAM) Consortium, 2024

Figure 10 - Yellow Duration Time Difference Between Controller and SPaT Message

This analysis module also generates a SPaT yellow phase performance analysis report of which an example is provided in APPENDIX C. In APPENDIX D, an example of generated SPaT yellow phase performance summary is report is provided.

APPENDIX A. Broadcast SPaT Message in JSON

The following shows an example of a converted SPaT message in PCAP to JSON in the Module 0 for processing by the subsequent verification and analysis modules in toolset. Starting with the UTC timestamp of packet capture, message id and flag to indicate 1609.2 security credential, the actual SPaT message follows in Table 2.

Table 2 - Converted Broadcast SPaT Message in PCAP to JSON

```
"Timestamp":1728694301467,"Direction":"RX","Message_id":19,"P1609dot2_flag":1,"Message":{"messageId":19,"value":{"intersections":[{"id":{"id":7706,"moy":410451,"name":"StateRte224&SunPeakDr","revision":103,"states":{"signalGroup":1,"state-time-speed":{"eventState":"permissive-Movement-Allowed","timing":{"maxEndTime":31296,"minEndTime":31296}}},{signalGroup":2,"state-time-speed":{"eventState":"protected-Movement-Allowed","timing":{"maxEndTime":31296,"minEndTime":31296}}},{signalGroup":3,"state-time-speed":{"eventState":"stop-And-Remain","timing":{"maxEndTime":31371,"minEndTime":31371}}},{signalGroup":4,"state-time-speed":{"eventState":"stop-And-Remain","timing":{"maxEndTime":32215,"minEndTime":32215}}},{signalGroup":5,"state-time-speed":{"eventState":"permissive-Movement-Allowed","timing":{"maxEndTime":31296,"minEndTime":31296}}},{signalGroup":6,"state-time-speed":{"eventState":"protected-Movement-Allowed","timing":{"maxEndTime":31296,"minEndTime":31296}}},{signalGroup":7,"state-time-speed":{"eventState":"stop-And-Remain","timing":{"maxEndTime":32215,"minEndTime":32215}}},{signalGroup":8,"state-time-speed":{"eventState":"stop-And-Remain","timing":{"maxEndTime":31371,"minEndTime":31371}}},{signalGroup":12,"state-time-speed":{"eventState":"permissive-Movement-Allowed","timing":{"maxEndTime":31296,"minEndTime":31296}}},{signalGroup":14,"state-time-speed":{"eventState":"stop-And-Remain","timing":{"maxEndTime":32215,"minEndTime":32215}}},{signalGroup":16,"state-time-speed":{"eventState":"permissive-Movement-Allowed","timing":{"maxEndTime":31296,"minEndTime":31296}}},{signalGroup":18,"state-time-speed":{"eventState":"stop-And-Remain","timing":{"maxEndTime":31371,"minEndTime":31371}}},{signalGroup":202,"state-time-speed":{"eventState":"protected-Movement-Allowed","timing":{"maxEndTime":31113,"minEndTime":31113}}},{signalGroup":204,"state-time-speed":{"eventState":"stop-And-Remain","timing":{"maxEndTime":32215,"minEndTime":32215}}},{signalGroup":206,"state-time-speed":{"eventState":"protected-Movement-Allowed","timing":{"maxEndTime":31163,"minEndTime":31163}}},{signalGroup":208,"state-time-speed":{"eventState":"stop-And-Remain","timing":{"maxEndTime":32215,"minEndTime":32215}}}], "status":"0430","timeStamp":41451},"timeStamp":410451}}
```


APPENDIX C. SPaT Yellow Phase Performance Analysis

Table 5 - SPaT Yellow Phase Performance Analysis

[illegible]

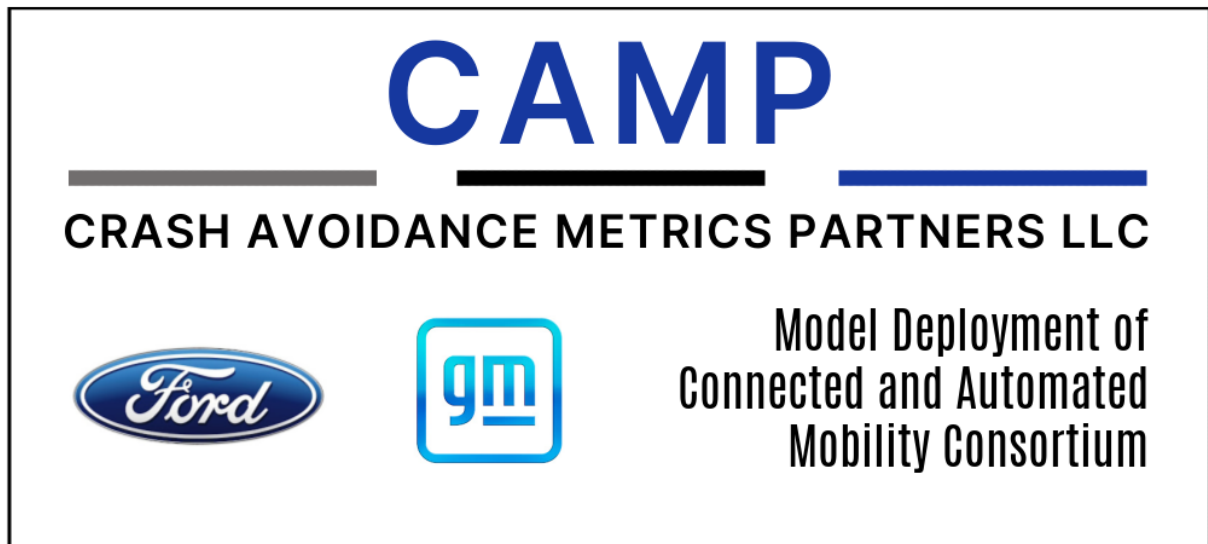
APPENDIX D. SPaT Yellow Phase Performance Summary Report

Table 6 - SPaT Yellow Phase Performance Summary Report

Test Name: SPaT - Test Location:		*** CI TSC & SPaT Message Yellow Phase Analysis Summary for RLW - v0.5 ***														
TSC Log: ATSPM		Report Created: 2024-10-22; 08:41:26														
TSC Log File: 7706-atspm.csv		Intersection ID: 7706														
SPaT File: 7706-ota-SPaT-0-7706.csv																
# of SPaT Messages Processed: 44998																
		<<<<<===== YP Processing Time Analysis: TSC to SPaT Broadcast =====>>>>>														
Signal		<----- TSC to SPaT Msg ----->			<----- RSU Msg Process (Jitter) ----->			<-End-to-End: TSC to SPaT Broadcast ->								
Group #		Max (ms)	Pass / Fail	Remark	Max (ms)	Pass / Fail	Remark	Max (ms)	Pass / Fail	Remark						
1		2757984	--Fail--	> 200ms	29	Pass		2758013	--Fail--	> 300ms						
2		19	Pass		29	Pass		45	Pass							
3			Pass			Pass			Pass							
4		20	Pass		29	Pass		45	Pass							
5		1047884	--Fail--	> 200ms	29	Pass		1047913	--Fail--	> 300ms						
6		19	Pass		29	Pass		45	Pass							
7			Pass			Pass			Pass							
8		20	Pass		29	Pass		45	Pass							
		<<<<<===== Yellow Phase Duration Analysis Panel =====>>>>>														
Signal		<----- TSC: YP Duration ----->					<----- SPaT: YP Duration (minEndTime @ Start) ----->					<----- SPaT: YP Duration at Msg Broadcast ----->				
Group #		Min (s)	Max (s)	Time Diff (s)	Pass / Fail	Remark	Msg Min (s)	Msg Max (s)	Time Diff (s)	Pass / Fail	Remark	RX Min (s)	RX Max (s)	Time Diff (s)	Pass / Fail	Remark
1		3.6	3.6	0	Pass		5.249	5.249	0	Pass		5.22	5.22	-0.029	Pass	
2		5.396	5.406	0.01	???	Unequal	5.246	39.849	34.603	--Fail--	> 200ms	5.22	39.833	34.587	--Fail--	> 200ms
3					Pass					Pass					Pass	
4		3.594	3.605	0.011	???	Unequal	3.445	3.45	0.005	Pass		3.42	3.434	-0.011	Pass	
5		4.3	4.3	0	Pass		5.249	5.249	0	Pass		5.22	5.22	-0.029	Pass	
6		5.396	5.406	0.01	???	Unequal	5.246	39.849	34.603	--Fail--	> 200ms	5.22	39.833	34.587	--Fail--	> 200ms
7					Pass					Pass					Pass	
8		3.594	3.605	0.011	???	Unequal	3.445	3.45	0.005	Pass		3.42	3.434	-0.011	Pass	
Notes:																
Following pass/fail criteria are used																
1. Yellow Phase Duration: Reported time difference between the TSC and the broadcast SPaT message > = 100ms																
2. RSU Process Time (Jitter): Reported time difference between the generated SPaT message time and message broadcast time > = 100ms																
3. Yellow Phase SPaT Broadcast Time: End-to-end time difference from TSC to SPaT message broadcast > 300ms (as per ITE CI guideline)																

Utah SMART Grant – Enabling Trust and Deployment Through Verified Connected Intersections Project

Assessing Node Point Accuracy in the SAE J2735 MAP Message



Produced by Crash Avoidance Metrics Partners LLC in response to the United States Department of Transportation Project entitled “Enabling Trust and Deployment Through Verified Connected Intersections under the SMART Grant program.

Report Documentation Page

Title and Subtitle Assessing Node Point Accuracy in the SAE J2735 MAP Message	Report Date August 2024
Author(s) Deering, R., Kumar, V., Parikh, J., VanSickle, S.	
Performing Organization Name and Address Crash Avoidance Metrics Partners LLC on behalf of the Model Deployment of Connected and Automated Mobility (MDCAM) Consortium 27220 Haggerty Road, Suite D-1 Farmington Hills, MI 48331	Contract or Grant Utah SMART Grant – Enabling Trust and Deployment Through Verified Connected Intersections Project under the SMART Grant program.
Abstract <p>The CTI 4501 Connected Intersection Implementation Guide [1] establishes requirements for SAE J2735 MAP Message node point accuracy supporting in-vehicle Red Light Violation Warning (RLVW) applications. These requirements are specified in relation to pavement markings defining ingress and egress lane boundaries for mapped intersections. Commercial Mobile Mapping services typically use a combination of scanning LiDAR technology in conjunction with high accuracy positioning (GNSS / GPS) and multi-axis high-resolution photography to create 3D models of roadways which include the locations of lane markings, curbs, stop bars and crosswalks. This information can be used to verify that the node point accuracy requirements established in CTI 4501 are satisfied by the MAP message developed for a Connected Intersection (CI). This paper describes the use of mobile LiDAR scan data to assess node point accuracy for three CIs located in southeast lower Michigan.</p>	
Key Words SAE J2735 MAP, RLVW, Mobile Mapping, Connected Intersection	

Table of Contents

Chapter 1.	Background.....	1
Chapter 2.	Assessment Data.....	2
	Intersection Selection.....	2
	Data Collection.....	4
Chapter 3.	Node Accuracy Analysis.....	6
	Position	6
	Lane Width	7
	Spacing on Curves.....	8
	Minimum Distance.....	9
Chapter 4.	MAP Analysis Reports	10
	Plymouth Road and Huron Parkway	10
	Moravian Drive and Garfield Road	14
	Moravian Drive and Metropolitan Parkway	18
Chapter 5.	Anomalies	21
Chapter 6.	Conclusions and Recommendations	23
APPENDIX A.	MAP Verification Data Collection.....	24
	Procedure.....	24
	Baseline Data.....	24
	Data Export Format.....	26
APPENDIX B.	Increased Accuracy Thresholds	28
	Plymouth Road and Huron Parkway ± 0.3 meters	28
	Plymouth Road and Huron Parkway ± 0.4 meters	32
	Moravian Drive and Garfield Road ± 0.3 meters	36
	Moravian Drive and Garfield Road ± 0.4 meters	39
	Moravian Drive and Metropolitan Parkway ± 0.3 meters	42
	Moravian Drive and Metropolitan Parkway ± 0.4 meters	44

Table of Tables

Table 1 - Analysis Report for Plymouth Road and Huron Parkway	10
Table 2 - Accuracy Report for Moravian Drive and Garfield Road	15
Table 3 - Analysis Report for Moravian Drive and Metropolitan Parkway	18
Table 4 - Data Element Format.....	26
Table 5 - Example Data Export File Configuration.....	26
Table 6 - Analysis Report for Plymouth Road and Huron Parkway \pm 0.3 Meters	28
Table 7 - Analysis Report for Plymouth Road and Huron Parkway \pm 0.4 Meters	32
Table 8 - Accuracy Report for Moravian Drive and Garfield Road \pm 0.3 Meters	36
Table 9 - Accuracy Report for Moravian Drive and Garfield Road \pm 0.4 Meters	39
Table 10 - Accuracy Report for Moravian Drive and Metropolitan Parkway \pm 0.3 Meters	42
Table 11 - Accuracy Report for Moravian Drive and Metropolitan Parkway \pm 0.4 Meters	44

Table of Figures

Figure 1 - Plymouth Road and Huron Parkway in Ann Arbor, MI	2
Figure 2 - Moravian Drive and Garfield Road in Macomb County, MI	3
Figure 3 - Moravian Drive and Metropolitan Parkway in Macomb County, MI	3
Figure 4 - Plymouth Road and Huron Parkway Data Export Illustration.....	4
Figure 5 - Moravian Drive and Garfield Road Data Export Illustration.....	5
Figure 6 - Moravian Drive and Metropolitan Parkway Data Export Illustration	5
Figure 7 - Node Position Analysis	7
Figure 8 - Lane Width Analysis	8
Figure 9 - Curve Radius Estimation	8
Figure 10 - Allowable Node Spacing Ranges	9
Figure 11 - MAP Analysis Illustration	9
Figure 12 - MAP Message Illustration for Plymouth Road and Huron Parkway	10
Figure 13 - MAP Message Illustration for Moravian Drive and Garfield Road.....	14
Figure 14 - MAP Message Illustration for Moravian Drive and Metropolitan Parkway	18
Figure 15 - Illustration of LiDAR Scanning Limitations	21
Figure 16 – Illustration of Lane Striping Practice for Curb Lanes	22
Figure 17 - Multi Lane Ingress Example	25
Figure 18 - Post Processing to Provide Continuous Representation	25
Figure 19 - Selection of Sequential Data Export Pairs	25
Figure 20 - Egress Lane Data Points	26

List of Acronyms and Definitions

Acronym	Meaning
CAMP	Crash Avoidance Metrics Partners LLC
CI	Connected Intersection
GPS	Global Positioning System
GNSS	Global Navigation Satellite System
IMU	Inertial Measurement Unit
LiDAR	Light Detection and Ranging
MAP	SAE J2735 Map Message
NAD83	North American Datum 1984
RLVW	Red Light Violation Warning
RTK	Real Time Kinetic
SAE	Society of Automotive Engineers
WGS84	World Geodetic System of 1983

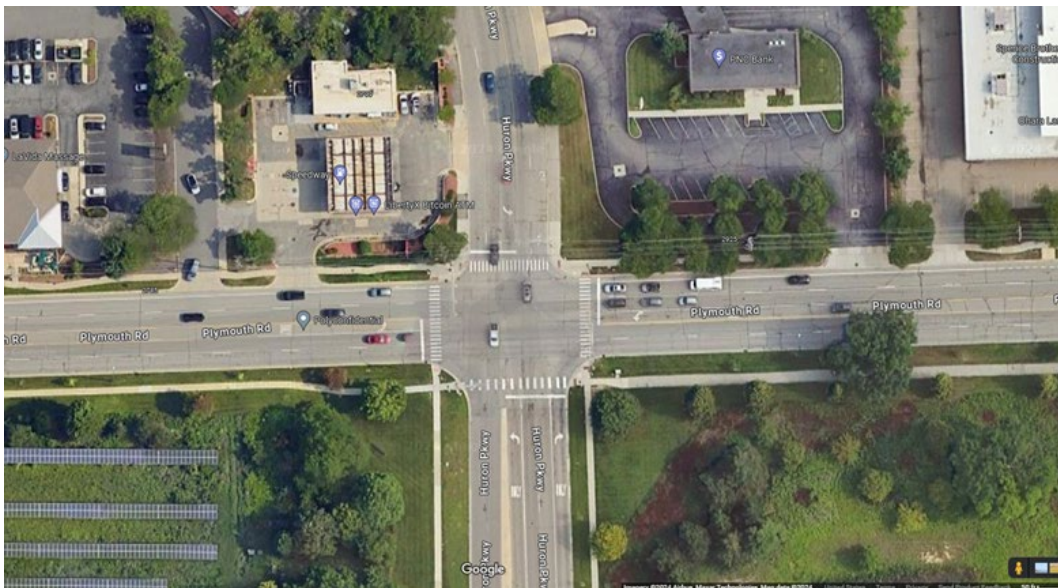
Chapter 1. Background

The CTI 4501 Connected Intersection Implementation Guide [1] establishes requirements for SAE J2735 MAP Message node point accuracy supporting in-vehicle Red Light Violation Warning (RLVW) applications. These requirements are specified in relation to pavement markings defining ingress and egress lane boundaries for mapped intersections. Commercial Mobile Mapping services typically use a combination of scanning LiDAR technology in conjunction with high accuracy positioning (GNSS / GPS) and multi-axis high-resolution photography to create 3D models of roadways which include the locations of lane markings, curbs, stop bars and crosswalks. This information can be used to verify that the node point accuracy requirements established in CTI 4501 are satisfied by the MAP message developed for a Connected Intersection (CI). This paper describes the use of mobile LiDAR scan data to assess node point accuracy for three CIs located in southeast lower Michigan.

Chapter 2. Assessment Data

Intersection Selection

The data export process specified in Appendix A was piloted using an existing 3D point cloud previously collected for the intersection of Plymouth Road and Huron Parkway in Ann Arbor, Michigan. The purpose of this initial exercise was for the Mobile Mapping service provider to develop the software modifications necessary to provide the export data file specified for analysis. The MAP message for this intersection was also created previously using mobile LiDAR data. However, subsequent road construction has altered the intersection. The MAP message has not yet been updated. This project collected new LiDAR data for the intersection to complete the assessment process. Thus, the final data export is not expected to exactly match the available MAP file for this intersection. This provides a negative test for the analysis software.



Source: Google Maps, Imagery ©2024 Airbus, Maxar Technologies, Map data©2024

Figure 1 - Plymouth Road and Huron Parkway in Ann Arbor, Michigan

LiDAR data was also collected at two intersections in Macomb County, Michigan. The intersections chosen encompass varying levels of complexity consisting of a two lane secondary road with some curvature crossing a major roadway followed by crossing a divided highway. These intersections are equipped with MAP messages created previously for the Macomb County Department of Roads from independent LiDAR survey data that match the current intersection configurations. These intersections are expected to provide a positive test for the analysis software.



Source: Google Maps, Imagery ©2024 Airbus, Maxar Technologies, Map data ©2024

Figure 2 - Moravian Drive and Garfield Road in Macomb County, Michigan



Source: Google Maps, Imagery ©2024 Airbus, Maxar Technologies, Map data ©2024

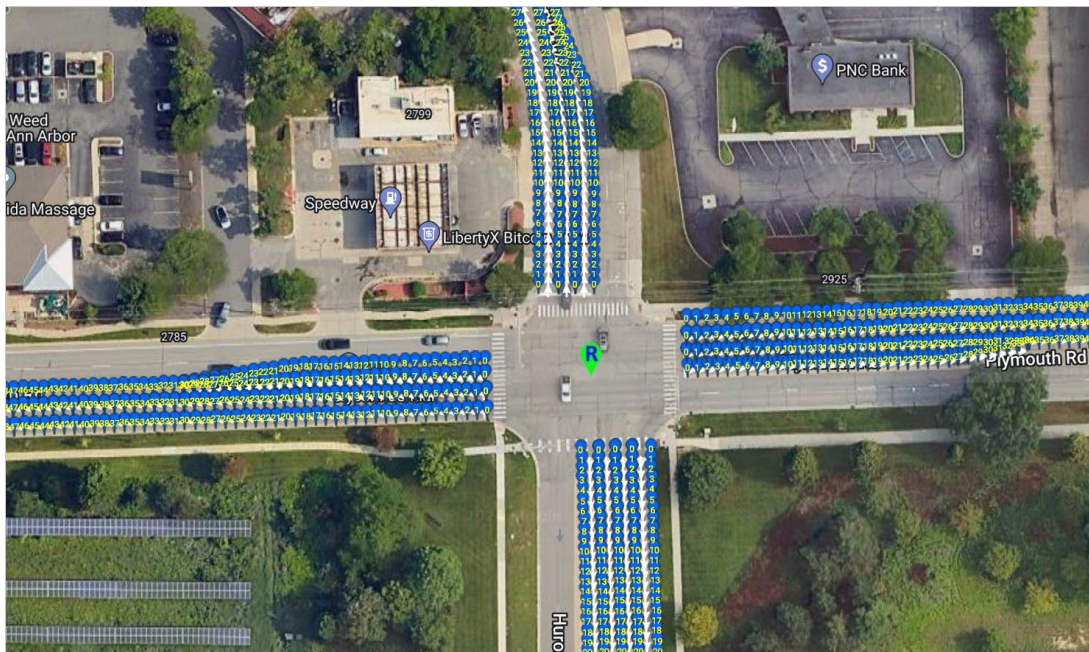
Figure 3 - Moravian Drive and Metropolitan Parkway in Macomb County, Michigan

Data Collection

Data was collected by a Mobile Mapping service provider following the MAP Verification Data Collection specification in Appendix A. A Trimble Mx9 Mobile Mapping Platform was utilized for data collection and analysis consisting of the following:

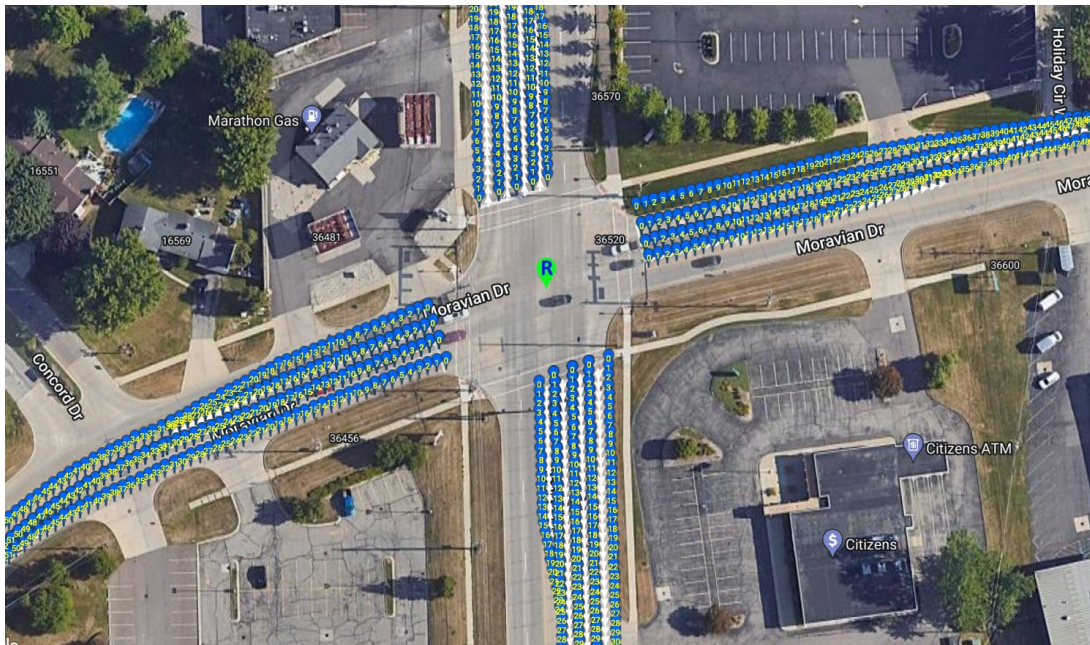
- Integrated dual pulse laser scan capable of accurate feature and asset collection from a high ground clearance vehicle at speeds approaching
- Multi-constellation Global Navigation Satellite System (GNSS) using Global Positioning System (GPS) antennas (primary and secondary)
- Integrated Inertia Measurement Unit (IMU)
- Integrated 5-axis LadyBug 5MP camera system
- Integrated control unit with 2TB SSD
- Data processing and position correction using Trimble Business Center software
- Positioning was augmented with L1, L2 and MI survey network Real Time Kinematic (RTK) data
- Reflective placards were placed along each intersection leg at surveyed locations to improve positioning accuracy in post processing

Data collection consisting of two runs at posted speed for each approach at both intersections, including system calibration and placement of location of reference markers, was accomplished in a single day. Testing was conducted during clear weather and at off peak traffic hours to reduce obscuration. Figure 4, Figure 5 and Figure 6 provide illustrations of the post processed Analysis Data Export for each intersection at a spacing on 2 meters. Estimated positional accuracy was $\pm 4\text{cm}$.



Source: Google Maps, Imagery ©2024 Airbus, Maxar Technologies, Map data©2024, – Data Overlay provided by CAMP Model Deployment of Connected and Automated Mobility Consortium, 2024

Figure 4 - Plymouth Road and Huron Parkway Data Export Illustration



Source: Google Maps, Imagery ©2024 Airbus, Maxar Technologies, Map data©2024, — Data Overlay provided by CAMP Model Deployment of Connected and Automated Mobility Consortium, 2024

Figure 5 - Moravian Drive and Garfield Road Data Export Illustration



Source: Google Maps, Imagery ©2024 Airbus, Maxar Technologies, Map data©2024, — Data Overlay provided by CAMP Model Deployment of Connected and Automated Mobility Consortium, 2024

Figure 6 - Moravian Drive and Metropolitan Parkway Data Export Illustration

Chapter 3. Node Accuracy Analysis

The accuracy requirements for MAP node points describing a CI ingress lane are specified in CTI 4051 v2 in terms of position, lane width, spacing on curves and total distance. These requirements and the means to assess the accuracy of MAP message content using information obtained from Mobile Mapping is illustrated in the following sections. Analysis software was developed to assess each of these accuracy requirements for each CI ingress lane using the Data Export Files obtained from Mobile Mapping as specified in APPENDIX A. MAP Verification Data Collection. The complete accuracy analysis for each CI is provided in Chapter 4 - MAP Analysis Reports.

Position

The combination of requirements 3.3.3.4.1.7 Center of Vehicle Lane Geometry, 3.3.3.4.1.11 First Node Point – Ingress Vehicle Lane and 3.3.3.4.1.22 Node Lane Width specify the accuracy of Node Point 0 as:

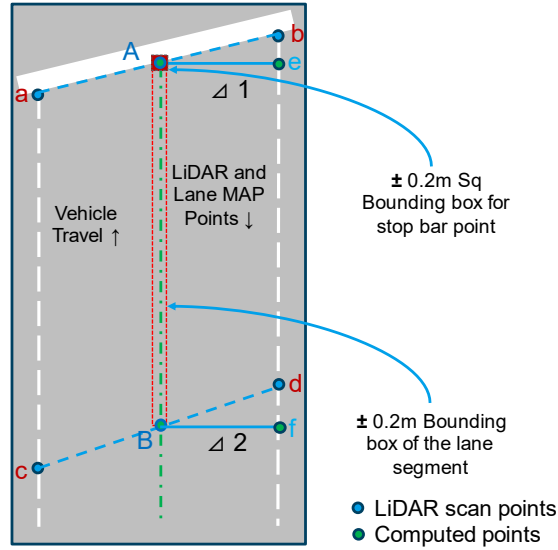
- ± 0.2 meters perpendicular to the lane centerline
- ± 0.2 meters along the lane centerline at the (leading) edge of the stop line
- ± 0.2 meters in elevation

Where “The lane center is the midpoint of a straight line perpendicular to the lane lines extended to the width of the lane.” (3.3.3.4.1.7) and “Lane width is the perpendicular distance between the center of the lane lines.” (3.3.3.4.1.22)

Requirement 3.3.3.4.1.7 Center of Vehicle Lane Geometry specifies the accuracy of Node Points 1 through n as:

- ± 0.2 meters perpendicular to the lane centerline
- ± 0.2 meters in elevation

The methodology used to examine the location of MAP Node Points is illustrated in Figure 7. Points a, b, c and d represent feature locations obtained from post processing the mobile mapping data. Point A is computed by averaging the locations of points a and b to determine the midpoint of line ab. Similarly point B is the calculated midpoint of line cd. Line AB then represents the calculated centerline of lane segment abcd with known heading angle. The bounding box which represents a valid location range in the horizontal plane for Node Point 0 is established ± 0.2 meters perpendicular to the lane centerline, ± 0.2 meters along the lane centerline at the leading edge of the stop line and ± 0.2 meters in elevation. For subsequent node points a bounding box is established along line AB ± 0.2 meters perpendicular to the lane centerline and ± 0.2 meters in elevation, which represents a valid location for any node points which may be located within lane segment abcd. This process is repeated for each lane segment defined by LiDAR scan points moving away from the stop bar.



Source: CAMP Model Deployment of Connected and Automated Mobility Consortium, 2024

Figure 7 - Node Position Analysis

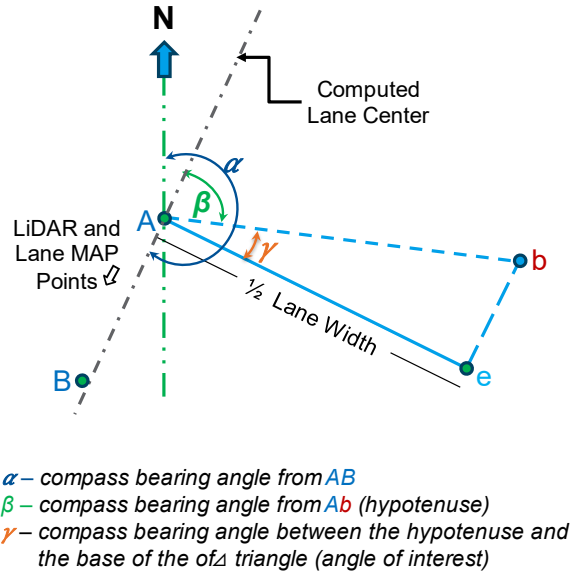
Lane Width

Requirements 3.3.3.4.1.5 Default Lane Width and 3.3.3.4.1.22 Node Lane Width specify the accuracy of all lane data reported as:

- ± 0.2 meters perpendicular to the lane lines

Figure 8 illustrates the methodology used to determine lane width, which has been defined as the perpendicular distance between lane lines. For this analysis, the effects of cross slope are assumed to be minimal. To calculate lane width at point A, consider a right triangle Abe from Figure 8 where Ae is the perpendicular distance between the right lane line and lane center. The compass bearing angle of line AB and line Ab are known from the locations of the endpoints¹. The angle of interest represented as γ in Figure 8 is computed as $\gamma = |\alpha - 90 - \beta|$. The length of line Ae represents $\frac{1}{2}$ lane width. Therefore, at point A the Lane Width = $2 * Ab * \cos(\gamma)$. This process is repeated at each midpoint along the calculated lane centerline. Interpolation within a lane segment may be necessary to assess MAP node points in sections of lane with varying width.

¹ Bearing Angle between Points 1 & 2 = $\text{atan2}(\sin(\text{long2}-\text{long1}).\cos(\text{lat2}), \cos(\text{lat1}).\sin(\text{lat2}) - \sin(\text{lat1}).\cos(\text{lat2}).\cos(\text{long2}-\text{long1}))$ radians



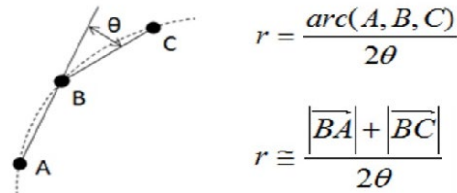
Source: CAMP Model Deployment of Connected and Automated Mobility Consortium, 2024

Figure 8 - Lane Width Analysis

Spacing on Curves

Requirement 3.3.3.4.1.20 Maximum Distance between Nodes specifies that nodes located along a curved section of roadway be placed such that the maximum distance between the actual centerline of a lane and a straight line between the two successive node points does not exceed 0.5 meters. Section 4.3.3.4.1.20 Maximum Distance between Nodes of CTI 4501 v2 also offers suggestions for estimating curvature based on heading angle change between successive node point pairs and calculating maximum allowable distance between node points based on this curvature estimate which have been implemented in the accuracy analysis software.

Figure 9 illustrates the curvature approximation technique where A, B and C represent nodes in the MAP. Lengths of map segments AB and BC and the change in compass bearing angle between the segments are determined from their position coordinates.



Source: CTI 4501v02 – work in progress

Figure 9 - Curve Radius Estimation

Figure 10 provides ranges of allowable node point spacing as a function of curve radius to satisfy the maximum node spacing requirement.

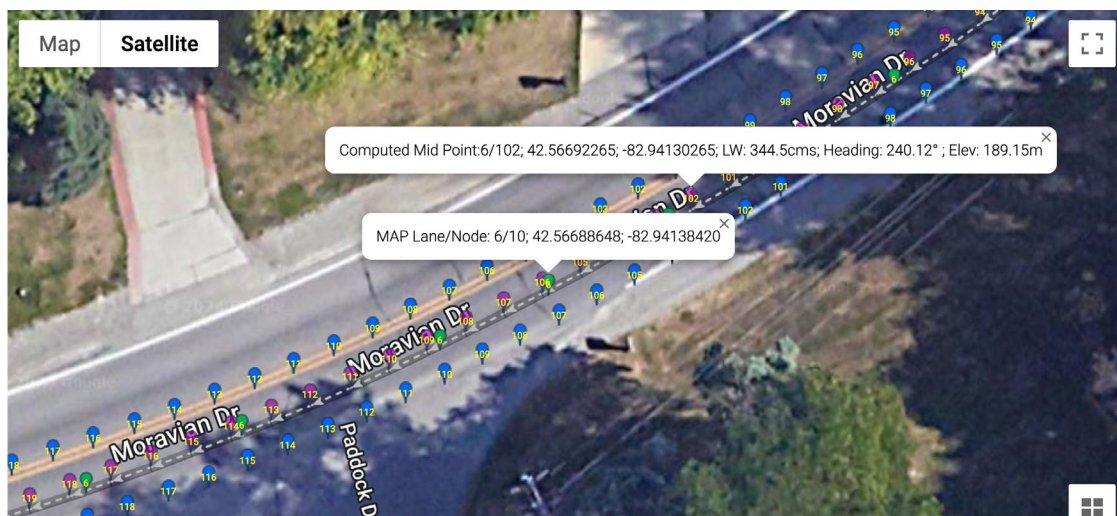
Radius of Curvature (m)	Distance (Range) Between Nodes (m)
< 100	15 – 20
101 to 200	22 – 30
201 to 300	25 – 35
301 to 400	30 – 38
401 to 500	32 – 45
501 to 600	35 – 52

Source: CTI 4501v02 – work in progress

Figure 10 - Allowable Node Spacing Ranges

Minimum Distance

Requirement 3.3.3.4.1.17 Advance Notification – Ingress Vehicle Lane sets the minimum distance from the stop line to the beginning of an ingress lane map (first to last node point) as 10 seconds of drive time at the 85th percentile speed for the roadway or a speed equal to the posted or statutory speed limit plus 7 miles per hour (mph). For distance in feet and speed in miles per hour, $D_{min} = (Posted\ Speed + 7) * 6.82$. For each ingress lane in the MAP message, total distance is calculated by summing the lengths of all the segments in comparison to D_{min} to assess this requirement.



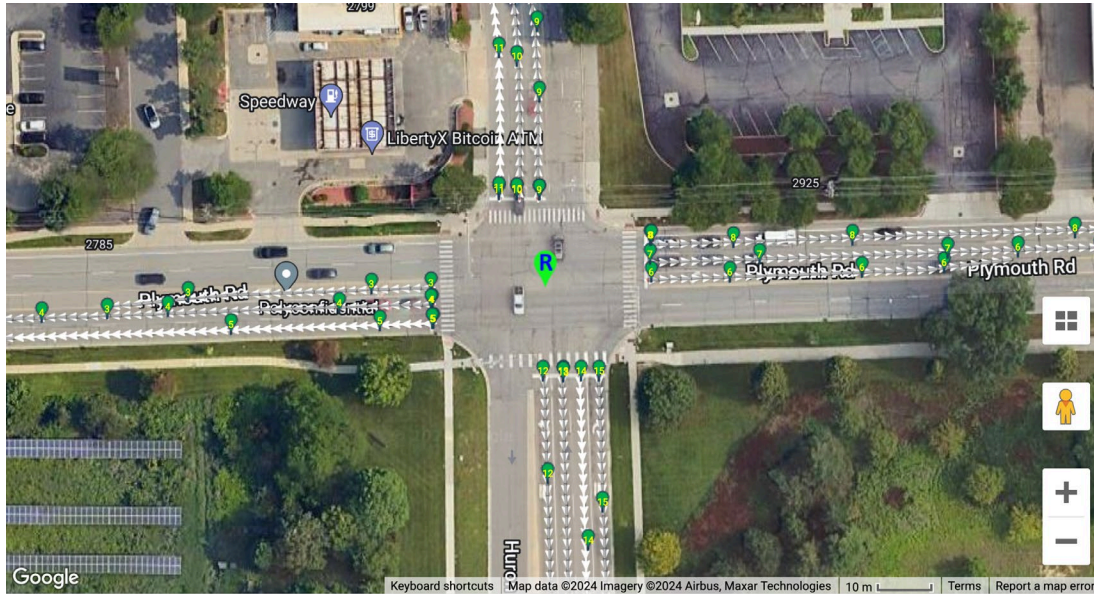
Source: Google Maps, Imagery ©2024 Airbus, Maxar Technologies, Map data©2024 - Data Overlay provided by CAMP Model Deployment of Connected and Automated Mobility Consortium, 2024

Figure 11 - MAP Analysis Illustration

Figure 11 illustrates a section of Moravian Drive ingress lane approaching Metropolitan Parkway with the Analysis Data Export points in blue identifying the lane lines, the calculated midpoint between each data pair shown in magenta with the lateral accuracy acceptance bounding box overlaid in grey, and the MAP node points superimposed in green. The calculated lane width, heading angle and elevation for the center point are also illustrated in the data balloon.

Chapter 4. MAP Analysis Reports

Plymouth Road and Huron Parkway



Source: Google Maps, Imagery ©2024 Airbus, Maxar Technologies, Map data©2024 - Data Overlay provided by CAMP Model Deployment of Connected and Automated Mobility Consortium, 2024

Figure 12 - MAP Message Illustration for Plymouth Road and Huron Parkway

Node accuracy analysis was performed on the data export for Plymouth Road and Huron Parkway following the procedures described in Chapter 3. An illustration of the MAP message for this intersection is provided in Figure 12 for Lane ID reference. The results of the analysis are provided in Table 1. The assessment of position accuracy is performed first for each node. If the position is not accurate to the specified criteria, no further assessments are performed for the node. In this case, only 11 out of 107 nodes evaluated passed the ± 0.2 meters criteria with none of the stop line nodes passing. In order to better understand the magnitude of node accuracy error at this intersection, the analysis was performed again using ± 0.3 meter and ± 0.4 meter criteria. The results are provided in Appendix B as Table 6 and Table 7, respectively, with limited improvement. At ± 0.3 meters, 17 of 107 nodes passed, and, at ± 0.4 meters, 22 of 107 nodes passed.

The MAP message for Plymouth and Huron is known to be out of date. It was generated by early mobile mapping techniques but completed prior to recent road reconstruction work performed on this intersection. Thus, the old MAP file is not expected to exactly match the new LiDAR scan.

Table 1 - Analysis Report for Plymouth Road and Huron Parkway

LiDAR Scan File: /Users/jsp-c/myStuff/MobiTel/CAMP (CV PFS + SOADS + UDOT Smart Grant)/UDOT - Smart Grant/MAP Assessment/AA Test/Plymouth Rd & Huron Pkwy_0619_2024.csv
Intersection Name: Plymouth Rd & Huron Pkwy, Ann Arbor, MI
Intersection Id: 81
Date/Time of LiDAR Scan Log Data: 2024-06-19 - 10:57:00
Date/Time of LiDAR Scan Log Data Processed: 2024-07-25 - 12:00:25

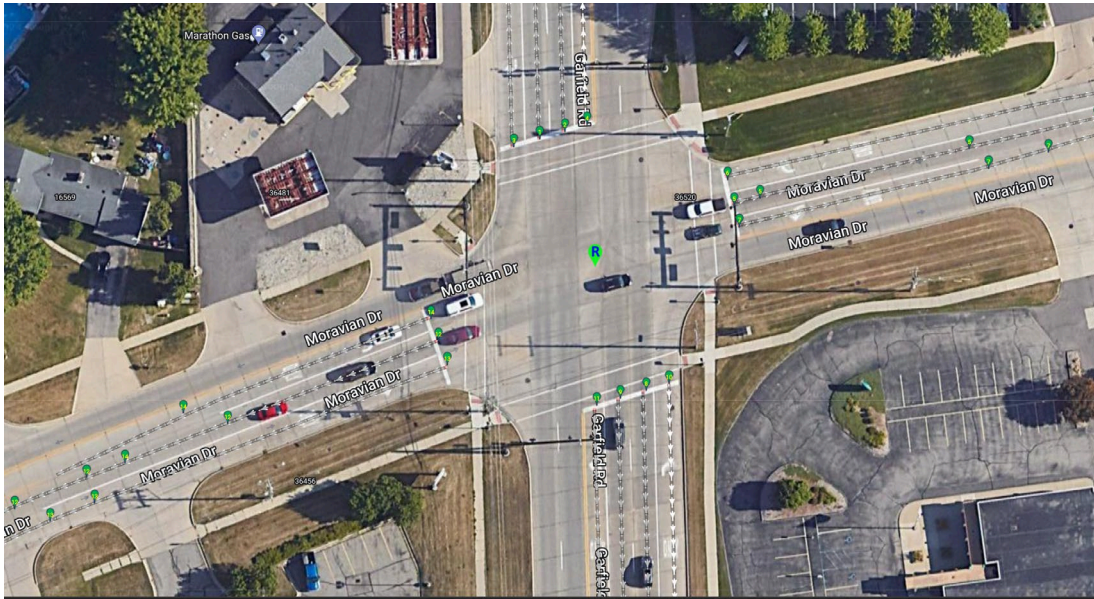
<<< START of MAP ASSESSMENT REPORT >>>						
Ingress	Node Pos	Lane Width	Altitude	Node Dist	Distance	
Lane Id	Node #	Accuracy	Accuracy	Accuracy	for Curve	Bet Node(m)
3	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
3	1	-- Fail --	-- NA --	-- NA --	-- NA --	11.01
3	2	-- Fail --	-- NA --	-- NA --	-- Fail --	34.19
3	3	-- Fail --	-- NA --	-- NA --	-- NA --	15.3
Mapped Lane Length:						60.5
4	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
4	1	-- Fail --	-- NA --	-- NA --	-- NA --	0.23
4	2	-- Fail --	-- NA --	-- NA --	-- NA --	16.9
4	3	-- Fail --	-- NA --	-- NA --	-- NA --	31.91
4	4	-- Fail --	-- NA --	-- NA --	-- NA --	23.36
4	5	-- Fail --	-- NA --	-- NA --	-- NA --	91.17
Mapped Lane Length:						163.57
5	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
5	1	-- Fail --	-- NA --	-- NA --	-- NA --	0.09
5	2	-- Fail --	-- NA --	-- NA --	-- NA --	9.7
5	3	-- Fail --	-- NA --	-- NA --	-- NA --	27.73
5	4	-- Fail --	-- NA --	-- NA --	-- NA --	44.83
5	5	-- Fail --	-- NA --	-- NA --	-- NA --	81.1
Mapped Lane Length:						163.44
6	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
6	1	-- Fail --	-- NA --	-- NA --	-- NA --	14.53
6	2	-- Fail --	-- NA --	-- NA --	-- NA --	24.5
6	3	-- Fail --	-- NA --	-- NA --	-- NA --	15.2
6	4	-- Fail --	-- NA --	-- NA --	-- NA --	13.96
Mapped Lane Length:						68.2
7	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
7	1	-- Fail --	-- NA --	-- NA --	-- NA --	20.26
7	2	-- Fail --	-- NA --	-- NA --	-- NA --	34.87
7	3	-- Fail --	-- NA --	-- NA --	-- NA --	28.07
7	4	-- Fail --	-- NA --	-- NA --	-- NA --	28.97
7	5	-- Fail --	-- NA --	-- NA --	-- NA --	23.04
7	6	-- Fail --	-- NA --	-- NA --	-- NA --	17.45

7	7	-- Fail --	-- NA --	-- NA --	-- NA --	15.95
7	8	-- Fail --	-- NA --	-- NA --	-- NA --	11.86
7	11	-- Fail --	-- NA --	-- NA --	-- NA --	17.97
7	12	-- Fail --	-- NA --	-- NA --	-- NA --	15.3
7	13	-- Fail --	-- NA --	-- NA --	-- NA --	18.79
7	14	-- Fail --	-- NA --	-- NA --	-- NA --	16.85
7	15	-- Fail --	-- NA --	-- NA --	-- NA --	20.57
7	16	-- Fail --	-- NA --	-- NA --	-- NA --	133.29
Mapped Lane Length:						430.85
8	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
8	1	-- Fail --	-- NA --	-- NA --	-- NA --	0.16
8	2	-- Fail --	-- NA --	-- NA --	-- NA --	15.39
8	3	-- Fail --	-- NA --	-- NA --	-- NA --	21.87
8	4	-- Fail --	-- NA --	-- NA --	-- NA --	41.37
8	5	-- Fail --	-- NA --	-- NA --	-- NA --	31.61
8	6	-- Fail --	-- NA --	-- NA --	-- NA --	37.82
8	7	-- Fail --	-- NA --	-- NA --	-- NA --	15.07
8	8	-- Fail --	-- NA --	-- NA --	-- NA --	14.78
8	9	-- Fail --	-- NA --	-- NA --	-- NA --	15.98
8	10	-- Fail --	-- NA --	-- NA --	-- NA --	12.21
8	11	-- Fail --	-- NA --	-- NA --	-- NA --	17.63
8	12	-- Fail --	-- NA --	-- NA --	-- NA --	18.03
8	13	-- Fail --	-- NA --	-- NA --	-- NA --	16.12
8	14	-- Fail --	-- NA --	-- NA --	-- NA --	36.66
8	15	-- Fail --	-- NA --	-- NA --	-- NA --	134.14
Mapped Lane Length:						428.85
9	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
9	1	-- Fail --	-- NA --	-- NA --	-- NA --	0.12
9	2	-- Pass --	-- Fail --	-- Fail --	-- Fail --	18.09
9	3	-- Fail --	-- NA --	-- NA --	-- NA --	13.04
9	4	-- Fail --	-- NA --	-- NA --	-- NA --	12.21
9	5	-- Fail --	-- NA --	-- NA --	-- NA --	10.93
9	6	-- Fail --	-- NA --	-- NA --	-- NA --	22.22
Mapped Lane Length:						76.62
10	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
10	1	-- Fail --	-- NA --	-- NA --	-- NA --	0.28
10	2	-- Fail --	-- NA --	-- NA --	-- Fail --	24.62

10	5	-- Fail --	-- NA --	-- NA --	-- NA --	11.52
10	6	-- Fail --	-- NA --	-- NA --	-- NA --	18.56
10	7	-- Fail --	-- NA --	-- NA --	-- NA --	15.96
10	8	-- Fail --	-- NA --	-- NA --	-- NA --	19.88
10	9	-- Fail --	-- NA --	-- NA --	-- NA --	15.35
10	10	-- Fail --	-- NA --	-- NA --	-- NA --	27.3
10	11	-- Fail --	-- NA --	-- NA --	-- NA --	123.56
Mapped Lane Length:						283.45
11	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
11	1	-- Fail --	-- NA --	-- NA --	-- NA --	0.46
11	2	-- Pass --	-- Fail --	-- Fail --	-- Fail --	25.81
11	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	12.18
11	4	-- Fail --	-- NA --	-- NA --	-- NA --	8.91
11	5	-- Fail --	-- NA --	-- NA --	-- NA --	10.78
11	6	-- Fail --	-- NA --	-- NA --	-- NA --	12.22
11	7	-- Fail --	-- NA --	-- NA --	-- NA --	13.96
11	8	-- Fail --	-- NA --	-- NA --	-- NA --	13.5
11	9	-- Fail --	-- NA --	-- NA --	-- NA --	13.75
Mapped Lane Length:						111.57
12	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
12	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	18.84
12	2	-- Fail --	-- NA --	-- NA --	-- NA --	60.77
12	3	-- Fail --	-- NA --	-- NA --	-- Fail --	43.57
12	4	-- Fail --	-- NA --	-- NA --	-- NA --	9.02
12	5	-- Fail --	-- NA --	-- NA --	-- NA --	8.77
Mapped Lane Length:						140.97
13	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
13	1	-- Fail --	-- NA --	-- NA --	-- NA --	0.04
13	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	50.7
13	3	-- Fail --	-- NA --	-- NA --	-- NA --	82.71
13	4	-- Pass --	-- Fail --	-- Fail --	-- NA --	19.28
13	5	-- Fail --	-- NA --	-- NA --	-- NA --	24.9
13	6	-- Fail --	-- NA --	-- NA --	-- NA --	72.05
Mapped Lane Length:						249.68
14	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	42.09
14	3	-- Fail --	-- NA --	-- NA --	-- NA --	48.33

14	4	-- Fail --	-- NA --	-- NA --	-- NA --	50.11
14	5	-- Fail --	-- NA --	-- NA --	-- NA --	77.08
Mapped Lane Length:						249
15	0	-- Pass --	-- Fail --	-- Fail --	-- NA --	0
15	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	24.17
15	2	-- Fail --	-- NA --	-- NA --	-- NA --	52.78
15	3	-- Fail --	-- NA --	-- NA --	-- Fail --	59
15	4	-- Fail --	-- NA --	-- NA --	-- NA --	28.89
Mapped Lane Length:						164.83
Pass		11				
Fail		96				

Moravian Drive and Garfield Road



Source: Google Maps, Imagery ©2024 Airbus, Maxar Technologies, Map data©2024 – Data Overlay provided by CAMP Model Deployment of Connected and Automated Mobility Consortium, 2024

Figure 13 - MAP Message Illustration for Moravian Drive and Garfield Road

Node accuracy analysis was performed on the data export for Moravian Drive and Garfield Road following the procedures described in Chapter 3. An illustration of the MAP message for this intersection is provided in Figure 13 for Lane ID reference. The results of the analysis are provided in Table 2. In this case, only 17 out of 69 nodes evaluated passed the ± 0.2 meters criteria with only one of the stop line nodes passing for Lane 10. In order to better understand the magnitude of node accuracy error at this intersection, the analysis was performed again using \pm meters 39 of 69 nodes passed.

The MAP message for this intersection was generated for Macomb County from a LiDAR scan performed by an independent contractor. The reference point in the broadcast message uses the NAD83 datum typical of stationary surveys rather than the WGS84 datum specified in SAE J2735. This results in a southeast shift in the data. The MAP Analysis Data export utilizes the WGS84 Datum as specified in APPENDIX A. Corrections were applied to the reference point to adjust to the correct datum before the MAP message for this intersection was analyzed. It was initially anticipated that the MAP for this intersection would be highly accurate. However the analysis report does not support this assumption. Further investigation into the process used to generate the MAP message from the stationary LiDAR scan as well as the reference point translation from NAD83 to WGS84 is needed.

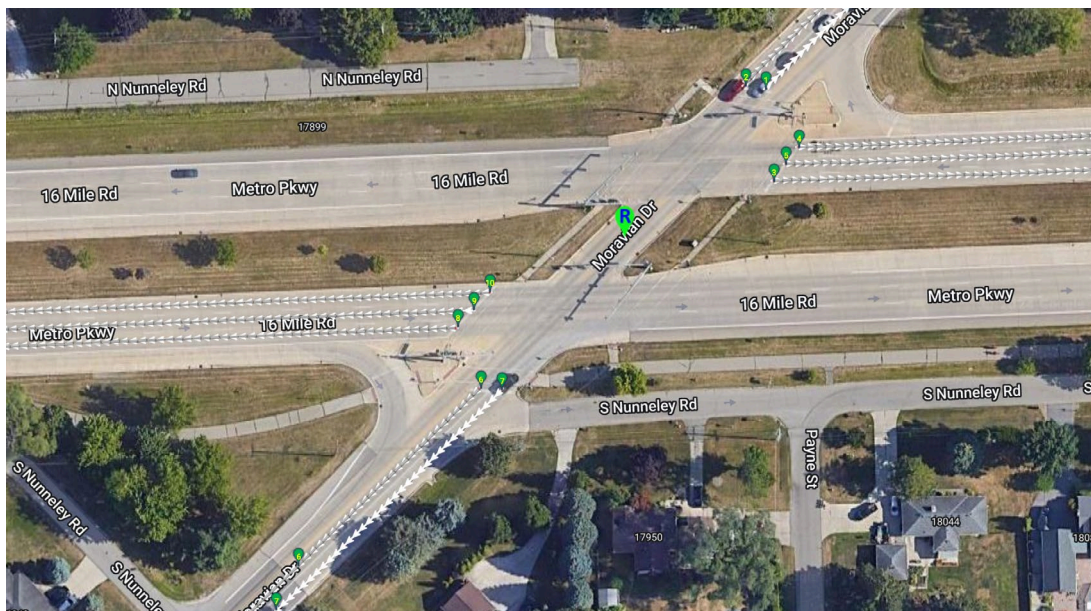
Table 2 - Accuracy Report for Moravian Drive and Garfield Road

Test Name: MAP Verification Based on LiDAR Scan						
LiDAR Scan File: /Users/jsp-c/myStuff/MobiTel/CAMP (CV PFS + SOADS + UDOT Smart Grant)/UDOT - Smart Grant/MAP Assessment/MCDR Test/Moravian_Garfield_0625_2024_revised.csv						
Intersection Name: Moravian Dr & Garfield Rd						
Intersection Id: 2515						
Date/Time of LiDAR Scan Log Data: 2024-05-09 - 10:18:38						
Date/Time of LiDAR Scan Log Data Processed: 2024-07-26 - 12:45:43						
<<< START of MAP ASSESSMENT REPORT >>>						
+/- 20cm						
Ingress		Node Pos	Lane Width	Altitude	Node Dist	Distance
Lane Id	Node #	Accuracy	Accuracy	Accuracy	for Curve	Bet Node(m)
1	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
1	1	-- Fail --	-- NA --	-- NA --	-- NA --	94.86
1	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	33.03
1	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	5.91
1	4	-- Pass --	-- Fail --	-- Fail --	-- NA --	55.25
1	5	-- Pass --	-- Fail --	-- Fail --	-- NA --	5.74
1	6	-- Pass --	-- NA --	-- Fail --	-- NA --	39.65
1	7	-- Fail --	-- NA --	-- NA --	-- NA --	36.41
Mapped Lane Length:						270.85
2	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
2	1	-- Fail --	-- NA --	-- NA --	-- NA --	269.91
Mapped Lane Length:						269.91
3	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
3	1	-- Fail --	-- NA --	-- NA --	-- Fail --	99.58
3	2	-- Fail --	-- NA --	-- NA --	-- NA --	29.54
Mapped Lane Length:						129.12
4	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
4	1	-- Fail --	-- NA --	-- NA --	-- Fail --	37.55

4	2	-- Fail --	-- NA --	-- NA --	-- NA --	7.63
Mapped Lane Length:						45.18
5	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
5	1	-- Fail --	-- NA --	-- NA --	-- NA --	4.07
5	2	-- Fail --	-- NA --	-- NA --	-- NA --	31.93
5	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	69.6
5	4	-- Pass --	-- Fail --	-- Fail --	-- NA --	67.12
5	5	-- Pass --	-- Fail --	-- Fail --	-- NA --	36.58
5	6	-- Fail --	-- NA --	-- NA --	-- NA --	66.88
Mapped Lane Length:						276.18
6	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
6	1	-- Fail --	-- NA --	-- NA --	-- NA --	68.29
6	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	10.91
6	3	-- Fail --	-- NA --	-- NA --	-- NA --	26.63
Mapped Lane Length:						105.83
7	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
7	1	-- Fail --	-- NA --	-- NA --	-- NA --	38.04
7	2	-- Fail --	-- NA --	-- NA --	-- NA --	9.2
7	3	-- Fail --	-- NA --	-- NA --	-- NA --	8.78
Mapped Lane Length:						56.02
8	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
8	1	-- Fail --	-- NA --	-- NA --	-- NA --	42.6
8	2	-- Fail --	-- NA --	-- NA --	-- NA --	25.83
8	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	30.4
8	4	-- Fail --	-- NA --	-- NA --	-- NA --	182.77
Mapped Lane Length:						281.6
9	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
9	1	-- Fail --	-- NA --	-- NA --	-- NA --	280.55
Mapped Lane Length:						280.55
10	0	-- Pass --	-- Fail --	-- Fail --	-- NA --	0
10	1	-- Pass --	-- Fail --	-- Fail --	-- Fail --	71.92
10	2	-- Fail --	-- NA --	-- NA --	-- NA --	9.12
10	3	-- Fail --	-- NA --	-- NA --	-- NA --	18.98
Mapped Lane Length:						100.02

11	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
11	1	-- Fail --	-- NA --	-- NA --	-- Fail --	37.44
11	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	3.25
11	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	1.48
11	4	-- Fail --	-- NA --	-- NA --	-- NA --	6.98
Mapped Lane Length:						49.15
12	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
12	1	-- Fail --	-- NA --	-- NA --	-- NA --	33.53
12	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	22.47
12	3	-- Fail --	-- NA --	-- NA --	-- NA --	11.61
12	4	-- Fail --	-- NA --	-- NA --	-- NA --	10.38
12	5	-- Fail --	-- NA --	-- NA --	-- NA --	6.72
12	6	-- Fail --	-- NA --	-- NA --	-- NA --	9.37
12	7	-- Fail --	-- NA --	-- NA --	-- NA --	6.78
12	8	-- Fail --	-- NA --	-- NA --	-- NA --	5.27
12	9	-- Fail --	-- NA --	-- NA --	-- NA --	7.71
12	10	-- Fail --	-- NA --	-- NA --	-- NA --	13.76
12	11	-- Fail --	-- NA --	-- NA --	-- NA --	14.11
12	12	-- Fail --	-- NA --	-- NA --	-- NA --	61.3
12	13	-- Fail --	-- NA --	-- NA --	-- NA --	55.98
Mapped Lane Length:						258.99
13	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
13	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	56.22
13	2	-- Fail --	-- NA --	-- NA --	-- NA --	7.11
13	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	13.2
13	4	-- Fail --	-- NA --	-- NA --	-- NA --	26.16
Mapped Lane Length:						102.69
14	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
14	1	-- Fail --	-- NA --	-- NA --	-- Fail --	39.28
14	2	-- Fail --	-- NA --	-- NA --	-- NA --	11.4
Mapped Lane Length:						50.68
Pass		17				
Fail		52				

Moravian Drive and Metropolitan Parkway



Source: Google Maps, Imagery ©2024 Airbus, Maxar Technologies, Map data©2024 – Data Overlay provided by CAMP Model Deployment of Connected and Automated Mobility Consortium, 2024

Figure 14 - MAP Message Illustration for Moravian Drive and Metropolitan Parkway

Node accuracy analysis was performed on the data export for Moravian Drive and Metropolitan Parkway following the procedures described in Chapter 3. An illustration of the MAP message for this intersection is provided in Figure 14 for Lane ID reference. The results of the analysis are provided in Table 3. In this case, only 13 out of 42 nodes evaluated passed the ± 0.2 meters criteria with only two of the stop line nodes passing for Lanes 9 and 10. In order to better understand the magnitude of node accuracy error at this intersection, the analysis was performed again using ± 0.3 meter and ± 0.4 meter criteria. The results are provided in Appendix B as Table 10 and Table 11, respectively, with limited improvement. At ± 0.3 meters, 26 of 42 nodes passed and, at ± 0.4 meters, 31 of 42 nodes passed.

Similar to the intersection of Moravian Drive and Garfield Road, the MAP message for this intersection was generated for Macomb County from a LiDAR scan performed by an independent contractor using the NAD83 datum. Corrections were applied to the reference point to adjust to the WGS84 datum before the MAP message was analyzed. It was initially anticipated that the MAP for this intersection would be highly accurate. However the analysis report does not support this assumption. Further investigation into the process used to generate the MAP message from the stationary LiDAR scan as well as the reference point translation from NAD83 to WGS84 is needed.

Table 3 - Analysis Report for Moravian Drive and Metropolitan Parkway

Test Name: MAP Verification Based on LiDAR Scan
 LiDAR Scan File: /Users/jsp-c/myStuff/MobiTel/CAMP (CV PFS + SOADS + UDOT Smart Grant)/UDOT - Smart Grant/MAP Assessment/MCDR Test/Moravian_Metro_0625_2024.csv

Intersection Name: Moravian Dr & Metro Pkwy

Intersection Id: 2347

Date/Time of LiDAR Scan Log Data: 2024-05-09 - 12:54:02

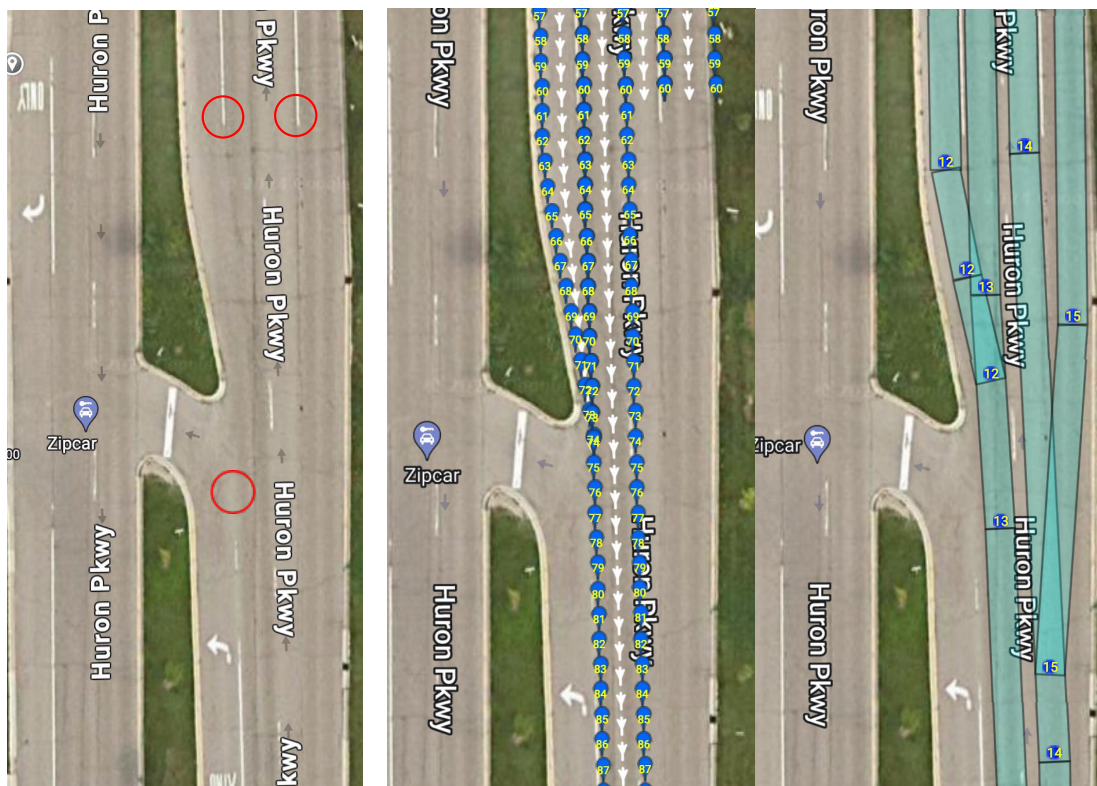
Date/Time of LiDAR Scan Log Data Processed: 2024-07-25 - 15:32:04

<<< START of MAP ASSESSMENT REPORT >>>						
+/- 20cm						
Ingress	Node Pos	Lane Width	Altitude	Node Dist	Distance	
Lane Id	Node #	Accuracy	Accuracy	Accuracy	for Curve	Bet Node(m)
1	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
1	1	-- Fail --	-- NA --	-- NA --	-- NA --	111.24
1	2	-- Fail --	-- NA --	-- NA --	-- NA --	53.48
1	3	-- Fail --	-- NA --	-- NA --	-- NA --	52.57
1	4	-- Fail --	-- NA --	-- NA --	-- NA --	24.51
Mapped Lane Length:						241.8
2	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
2	1	-- Fail --	-- NA --	-- NA --	-- Fail --	65.21
2	2	-- Fail --	-- NA --	-- NA --	-- NA --	40.33
Mapped Lane Length:						105.54
3	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
3	1	-- Fail --	-- NA --	-- NA --	-- NA --	181.28
3	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	75.26
Mapped Lane Length:						256.54
4	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
4	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	248.7
Mapped Lane Length:						248.7
5	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
5	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	253.56
Mapped Lane Length:						253.56
6	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
6	1	-- Fail --	-- NA --	-- NA --	-- NA --	55.6
6	2	-- Fail --	-- NA --	-- NA --	-- NA --	61.76
6	3	-- Fail --	-- NA --	-- NA --	-- NA --	27.82
6	4	-- Fail --	-- NA --	-- NA --	-- NA --	19.06
6	5	-- Fail --	-- NA --	-- NA --	-- NA --	7.28
6	6	-- Fail --	-- NA --	-- NA --	-- NA --	5.12
6	7	-- Fail --	-- NA --	-- NA --	-- NA --	9.5
6	8	-- Fail --	-- NA --	-- NA --	-- NA --	6.82
6	9	-- Fail --	-- NA --	-- NA --	-- NA --	12.3
6	10	-- Fail --	-- NA --	-- NA --	-- NA --	6.43

6	11	-- Fail --	-- NA --	-- NA --	-- NA --	5.67
6	12	-- Pass --	-- Fail --	-- Fail --	-- NA --	10.02
6	13	-- Pass --	-- Fail --	-- Fail --	-- NA --	7.75
6	14	-- Fail --	-- NA --	-- NA --	-- NA --	12.32
Mapped Lane Length:						247.45
7	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
7	1	-- Pass --	-- Fail --	-- NA --	-- NA --	69.14
7	2	-- Fail --	-- NA --	-- NA --	-- NA --	26.24
7	3	-- Fail --	-- NA --	-- NA --	-- NA --	33.53
Mapped Lane Length:						128.91
8	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
8	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	260.97
Mapped Lane Length:						260.97
9	0	-- Pass --	-- Fail --	-- NA --	-- NA --	0
9	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	239.71
9	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	25.26
Mapped Lane Length:						264.97
10	0	-- Pass --	-- Fail --	-- NA --	-- NA --	0
10	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	243.3
10	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	25.43
Mapped Lane Length:						268.73
Pass		13				
Fail		29				

Chapter 5. Anomalies

As described in APPENDIX A – MAP Verification Data Collection, the data processing software provided by the mobile mapping system supplier includes functions to extract features of interest such as lane lines from the 3D point cloud as well as bridge small gaps in lane lines created by driveways, smooth dashed lines into continuous functions for analysis and extend lane lines to identify the intersection with the stop line. There are, however, real-world situations requiring expert judgement regarding the appropriate use of such functionality. Consider the north bound ingress lanes on Huron Parkway approaching Plymouth Road shown in Figure 15.



Source: Google Maps, Imagery ©2024 Airbus, Maxar Technologies, Map data©2024 – Data Overlay provided by CAMP Model Deployment of Connected and Automated Mobility Consortium, 2024

Figure 15 - Illustration of LiDAR Scanning Limitations

The addition of the left turn lane on Huron Parkway at Plymouth Road, the presence of a tee intersection on the approach with its own left turn lane, and the extremely long taper into the right turn lane added for Plymouth Road (> 100m) create several conditions requiring expert interpretation in data reduction. The left image in Figure 15 shows the gaps in ingress lane lines approaching Plymouth Road. The middle image in Figure 15 adds the LiDAR scan data export points at 2 meter spacing starting at the stop line. In this analysis, the data reduction software was used to extend the lane left lane line of the left through from the break point where the left turn lane taper at Plymouth Road completes to the point where the line terminates do to the tee intersection, enabling analysis of this section of the left through lane. However, this was not done for the right side of the right through lane because there is no specific physical location identified by the LiDAR scan to locate the endpoint of such an extension. The right side of this through lane is formed by a curb and the inflection point where the taper begins is not distinct. Such an extension may be inaccurate for long distances, especially on curved road segments. The right image in Figure 15 shows segments of the broadcast MAP message for this intersection. The gap in analysis data limits the

ability to assess the accuracy of some MAP segments on the right through lane (Lane ID14) and right turn lane (Lane ID 15) for this CI.

Figure 16 provides another illustration of how lane striping practices impact the MAP message. The data export points from the LiDAR scan of the east bound ingress lanes on Metropolitan Parkway approaching Moravian Drive are shown. Typical practice for the intersections evaluated in Macomb is to paint an outer edge line for lane segments with a shoulder but no curb and not paint an outer edge line where there is a curb in close proximity to the lane edge. This makes the outer edge of the left most ingress lane the curb location causing the width of this lane to vary from the default value that describes the other ingress lanes. This variation was not reflected in the MAP message for this intersection.



Figure 16 – Illustration of Lane Striping Practice for Curb Lanes

Chapter 6. Conclusions and Recommendations

3D LiDAR Point Clouds obtained from Mobile Mapping of three CIs located in southeast lower Michigan were post processed to obtain data describing the locations of the lane markings, curbs and stop bars. This information was then used to assess the accuracy of the MAP node points broadcast for these intersections. Criteria for node point accuracy relative to lane marking locations are provided in CTI 4501v2 for position, elevation, lane width and spacing on curves. The result is a pass / fail evaluation report for each intersection.

The technique developed provides a viable approach to assessing MAP node point accuracy. However, some limitations were identified requiring expert judgement in post processing for specific situations such as the initiation of dedicated turn lanes and intersection approaches that contain other intersections. Additional field experience is needed to better understand the extent of these limitations and establish best practices to address gaps in LiDAR data.

The analysis of two intersections expected to perform well resulted in most node points failing requirements. Increasing the error tolerances applied during analysis provided some improvement in performance, but not to the levels expected. These were MAPs generated from stationary LiDAR survey data by a third party vendor. The messages were obtained for analysis from the CI broadcasts. The exact process by which these node points were generated from stationary LiDAR data is unknown. In addition, the reference points broadcast for these intersections incorrectly use the NAD83 datum. It was necessary to convert to WGS84 to perform analysis. Thus the absolute accuracy of the MAP data for these CIs appears uncertain.

Final verification of the node point accuracy tools and techniques developed here should be performed using a 'reference intersection' or series of intersections. The positions of key lane markings should be independently surveyed to provide a means to confirm the accuracy of Mobile Mapping data and validity of the analysis approach proposed.

APPENDIX A. MAP Verification Data Collection

Procedure

The road scanning service provider will drive each approach of the connected intersection under evaluation and collect, at a minimum, the data described below for each through lane. Ideally, all adjacent through lanes should be mapped simultaneously. However, if the total approach is too wide, or to minimize potential occlusion from adjacent traffic, multiple scans are acceptable to generate a composite data model of each approach.

Scanning should begin at a distance slightly farther away from the stop line than required by the advanced notification range identified in CTI 4501² and terminate after establishing the location of the first broken line segment in the corresponding egress lane(s). The instrumented vehicle should be driven in accordance with local laws.

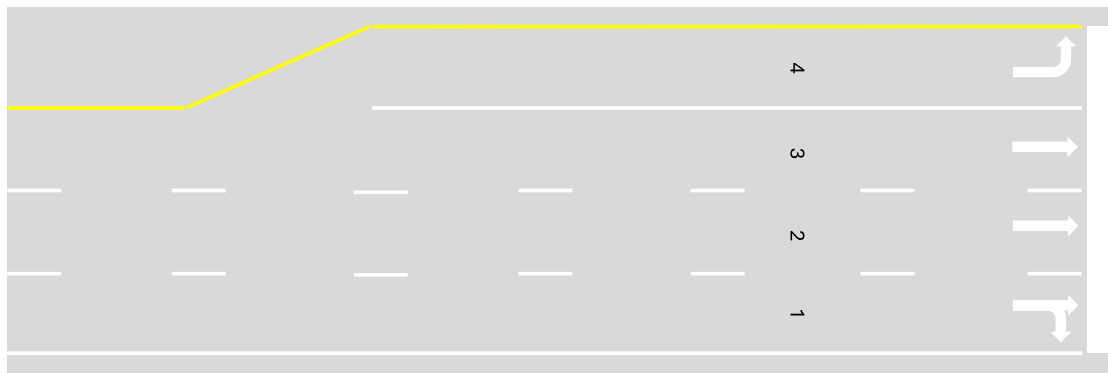
The horizontal accuracy of the location data provided should be ± 4 cm or better and support the ability to identify, measure and extract the lane line widths from the data model. The vertical accuracy of the location data should be ± 8 cm or better. The use of surveyed reference markers as part of data collection to verify positional accuracy is encouraged.

Baseline Data

Data post processing and export for use in MAP node accuracy analysis is illustrated for a multi-lane signalized intersection depicted in Figure 17.

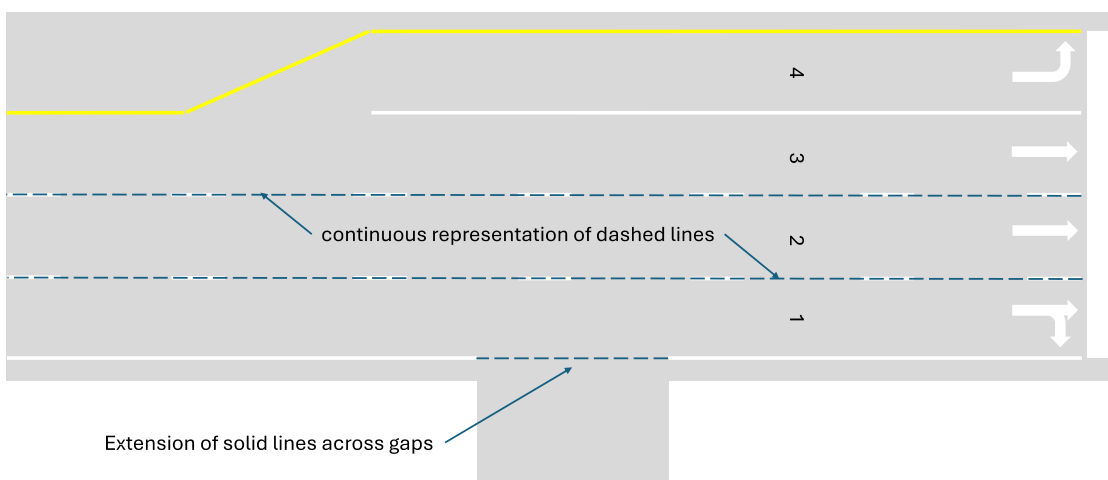
- LiDAR scan data should be collected for the distance provided in the intersection MAP message, which is at least the advance notification range. An estimate of positional accuracy should be included with each data set collected.
- The LiDAR data is post processed to extract the locations of the lane boundaries represented by lane lines, the stop bar and, if present, the pedestrian crosswalks for both ingress and egress. In the absence of lane edge lines, the use of pavement edges / transitions or curbs may be reported as appropriate.
- Commercially available LiDAR data analysis software typically provides functionality to represent dashed lane lines as continuous functions and fill in gaps in lane edge lines caused by driveways and small crossroads as illustrated in Figure 18.
- Data pairs representing the edges of each approach lane should be exported beginning at the leading edge of the stop bar and extending away from the intersection. These pairs should be indexed to the lane ids used in the MAP message.
- Maximum spacing between data pairs should be no greater than two meters to ensure reasonable representation of line end points. Figure 19 illustrates missing line end point information caused by excessive spacing. Alternatively, if lane line end points can be separately identified and reported, larger spacing may be considered for straight road segments.
- To minimize sample induced errors when assessing node spacing on curved roads, data should be reported at spacings ranging from 2 meters for a 100 m radius curve and increasing to 6 m for a 900 m radius curve. (SAE J3238/2 – in process)
- Unpaired data may occur due to gaps in lane lines in transitions such as tapers to add additional lanes as illustrated in Figure 19. In such cases the unpaired data export should still be reported.
- Single data point pairs should also be reported for each egress lane at the trailing edge of the pedestrian walkway, if present, as illustrated in Figure 20.

² Minimum MAP distance required is equivalent to ten seconds of drive time at the posted speed limit plus 7 mph.



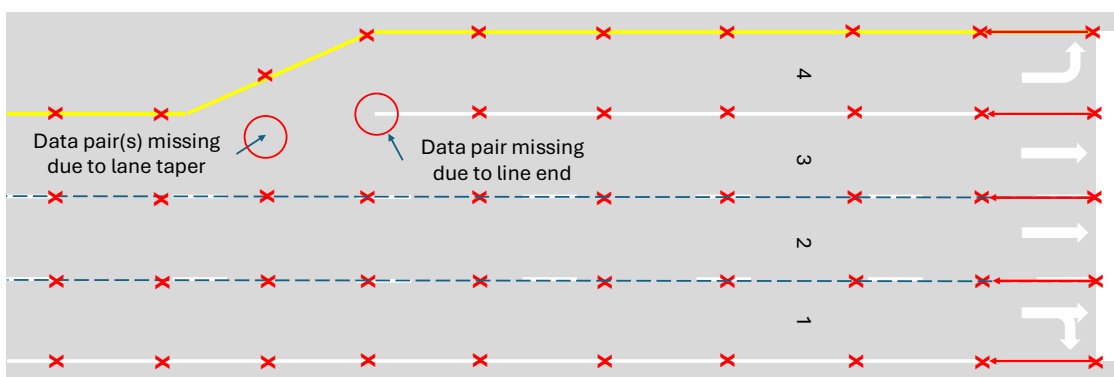
Source: CAMP Model Deployment of Connected and Automated Mobility Consortium, 2024

Figure 17 - Multi Lane Ingress Example



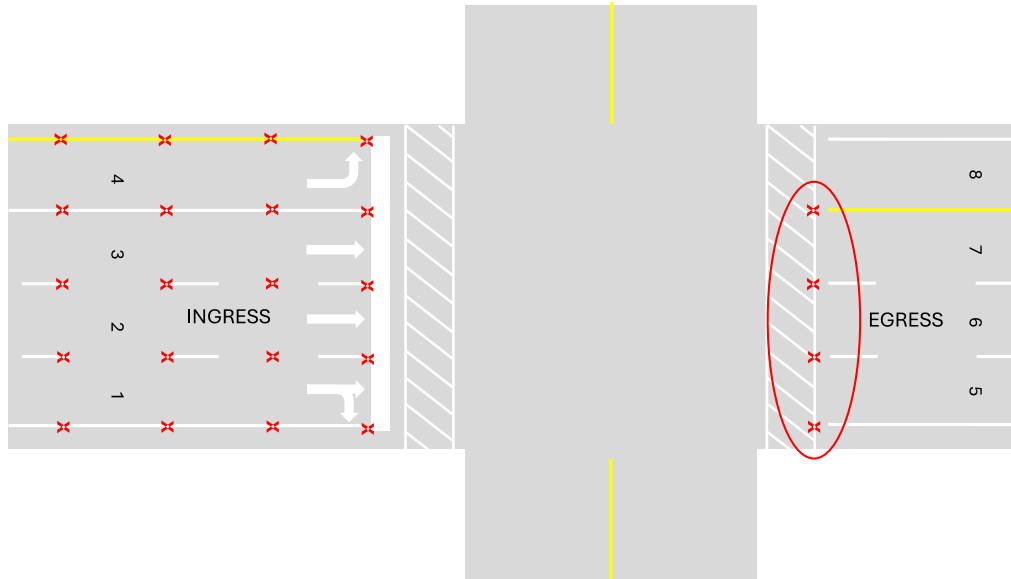
Source: CAMP Model Deployment of Connected and Automated Mobility Consortium, 2024

Figure 18 - Post Processing to Provide Continuous Representation



Source: CAMP Model Deployment of Connected and Automated Mobility Consortium, 2024

Figure 19 - Selection of Sequential Data Export Pairs



Source: CAMP Model Deployment of Connected and Automated Mobility Consortium, 2024

Figure 20 - Egress Lane Data Points

Data Export Format

The output data should be provided in CSV format containing the elements illustrated in Table 4 for each ingress lane. Data elements should conform to the format specified in Table 5.

Table 4 - Data Element Format

Data Element	Format
Intersection ID	Integer (Road Authority ID will replace)
Intersection Name	String
Lane Type	Ingress, Egress, Xwalk
MAP Lane Id	Integer
Sequence Number	Integer
Lane Line Position Points	WGS 84 Datum
- latitude – Left edge, Right edge	degrees (7 decimal)
- longitude – Left edge, Right edge	degrees (7 decimal)
- elevation – Left edge, Right edge	meters (1 decimal)
Lane marker type	Lane, Crosswalk
Distance to Stop bar (Point 0)	Meters (2 decimal)

Table 5 - Example Data Export File Configuration

Intersection ID:	Integer (Future – Road Authority ID (RAID) format)
Intersection Name:	String
Scan Date/Time:	yyyy-mm-dd – hh:mm:ss

Lane Type	Lane ID	Seq #	Lat_1	Lon_1	Elev_1	Lat_2	Lon_2	Elev_2	Dist. to SB	Lane Mark
Ingress	1	0	Lat1	Lon1	Elev1	Lat2	Lon2	Elev2	Dist	Lane
Ingress	1	1	Lat1	Lon1	Elev1	Lat2	Lon2	Elev2	Dist	Lane
Ingress	1	2	Lat1	Lon1	Elev1	Lat2	Lon2	Elev2	Dist	Lane
Ingress	1	3	Lat1	Lon1	Elev1	Lat2	Lon2	Elev2	Dist	Lane
...
Ingress	2	0	Lat1	Lon1	Elev1	Lat2	Lon2	Elev2	Dist	Lane

Appendix A: MAP Verification Data Collection

Ingress	2	1	Lat1	Lon1	Elev1	Lat2	Lon2	Elev2	Dist	Lane
Ingress	2	2	Lat1	Lon1	Elev1	Lat2	Lon2	Elev2	Dist	Lane
Ingress	2	3	Lat1	Lon1	Elev1	Lat2	Lon2	Elev2	Dist	Lane
...
Egress	3	0	Lat1	Lon1	Elev1	Lat2	Lon2	Elev2	Dist	Xwalk
Egress	3	1	Lat1	Lon1	Elev1	Lat2	Lon2	Elev2	Dist	Xwalk
Egress	3	2	Lat1	Lon1	Elev1	Lat2	Lon2	Elev2	Dist	Xwalk
Egress	3	3	Lat1	Lon1	Elev1	Lat2	Lon2	Elev2	Dist	Xwalk
...
Ingress	4	0	Lat1	Lon1	Elev1	Lat2	Lon2	Elev2	Dist	Lane
Ingress	4	1	Lat1	Lon1	Elev1	Lat2	Lon2	Elev2	Dist	Lane
Ingress	4	2	Lat1	Lon1	Elev1	Lat2	Lon2	Elev2	Dist	Lane
Ingress	4	3	Lat1	Lon1	Elev1	Lat2	Lon2	Elev2	Dist	Lane
...

APPENDIX B. Increased Accuracy Thresholds

Plymouth Road and Huron Parkway ± 0.3 Meters

Table 6 - Analysis Report for Plymouth Road and Huron Parkway ± 0.3 Meters

<<< START of MAP ASSESSMENT REPORT >>>						
Ingress	Node Pos	Lane Width	Altitude	Node Dist	Distance	
Lane Id	Node #	Accuracy	Accuracy	Accuracy	for Curve	Bet Node(m)
3	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
3	1	-- Fail --	-- NA --	-- NA --	-- NA --	11.01
3	2	-- Fail --	-- NA --	-- NA --	-- Fail --	34.19
3	3	-- Fail --	-- NA --	-- NA --	-- NA --	15.3
Mapped Lane Length:						60.5
4	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
4	1	-- Fail --	-- NA --	-- NA --	-- NA --	0.23
4	2	-- Fail --	-- NA --	-- NA --	-- NA --	16.9
4	3	-- Fail --	-- NA --	-- NA --	-- NA --	31.91
4	4	-- Fail --	-- NA --	-- NA --	-- NA --	23.36
4	5	-- Fail --	-- NA --	-- NA --	-- NA --	91.17
Mapped Lane Length:						163.57
5	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
5	1	-- Fail --	-- NA --	-- NA --	-- NA --	0.09
5	2	-- Fail --	-- NA --	-- NA --	-- NA --	9.7
5	3	-- Fail --	-- NA --	-- NA --	-- NA --	27.73
5	4	-- Fail --	-- NA --	-- NA --	-- NA --	44.83
5	5	-- Fail --	-- NA --	-- NA --	-- NA --	81.1
Mapped Lane Length:						163.45
6	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
6	1	-- Fail --	-- NA --	-- NA --	-- NA --	14.53
6	2	-- Fail --	-- NA --	-- NA --	-- NA --	24.5
6	3	-- Fail --	-- NA --	-- NA --	-- NA --	15.2
6	4	-- Fail --	-- NA --	-- NA --	-- NA --	13.96
Mapped Lane Length:						68.19
7	0	-- Fail --	-- NA --	-- NA --	-- NA --	0

Appendix B: Increased Accuracy Thresholds

7	1	-- Fail --	-- NA --	-- NA --	-- NA --	20.26
7	2	-- Fail --	-- NA --	-- NA --	-- NA --	34.87
7	3	-- Fail --	-- NA --	-- NA --	-- NA --	28.07
7	4	-- Fail --	-- NA --	-- NA --	-- NA --	28.97
7	5	-- Fail --	-- NA --	-- NA --	-- NA --	23.04
7	6	-- Fail --	-- NA --	-- NA --	-- NA --	17.45
7	7	-- Fail --	-- NA --	-- NA --	-- NA --	15.95
7	8	-- Fail --	-- NA --	-- NA --	-- NA --	11.86
7	9	-- Fail --	-- NA --	-- NA --	-- NA --	12.74
7	10	-- Fail --	-- NA --	-- NA --	-- NA --	14.88
7	11	-- Fail --	-- NA --	-- NA --	-- NA --	17.97
7	12	-- Fail --	-- NA --	-- NA --	-- NA --	15.3
7	13	-- Fail --	-- NA --	-- NA --	-- NA --	18.79
7	14	-- Fail --	-- NA --	-- NA --	-- NA --	16.85
7	15	-- Fail --	-- NA --	-- NA --	-- NA --	20.57
7	16	-- Fail --	-- NA --	-- NA --	-- NA --	133.29
Mapped Lane Length:						430.86
8	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
8	1	-- Fail --	-- NA --	-- NA --	-- NA --	0.16
8	2	-- Fail --	-- NA --	-- NA --	-- NA --	15.39
8	3	-- Fail --	-- NA --	-- NA --	-- NA --	21.87
8	4	-- Fail --	-- NA --	-- NA --	-- NA --	41.37
8	5	-- Fail --	-- NA --	-- NA --	-- NA --	31.61
8	6	-- Fail --	-- NA --	-- NA --	-- NA --	37.82
8	7	-- Fail --	-- NA --	-- NA --	-- NA --	15.07
8	8	-- Fail --	-- NA --	-- NA --	-- NA --	14.78
8	9	-- Fail --	-- NA --	-- NA --	-- NA --	15.98
8	10	-- Fail --	-- NA --	-- NA --	-- NA --	12.21
8	11	-- Fail --	-- NA --	-- NA --	-- NA --	17.63
8	12	-- Fail --	-- NA --	-- NA --	-- NA --	18.03
8	13	-- Fail --	-- NA --	-- NA --	-- NA --	16.12
8	14	-- Fail --	-- NA --	-- NA --	-- NA --	36.66
8	15	-- Fail --	-- NA --	-- NA --	-- NA --	134.14
Mapped Lane Length:						428.84
9	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
9	1	-- Fail --	-- NA --	-- NA --	-- NA --	0.12
9	2	-- Pass --	-- Fail --	-- Fail --	-- Fail --	18.09
9	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	13.04

Appendix B: Increased Accuracy Thresholds

9	4	-- Fail --	-- NA --	-- NA --	-- NA --	12.21
9	5	-- Fail --	-- NA --	-- NA --	-- NA --	10.93
9	6	-- Fail --	-- NA --	-- NA --	-- NA --	22.22
Mapped Lane Length:						76.61
10	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
10	1	-- Fail --	-- NA --	-- NA --	-- NA --	0.28
10	2	-- Fail --	-- NA --	-- NA --	-- Fail --	24.62
10	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	14.25
10	4	-- Fail --	-- NA --	-- NA --	-- NA --	12.18
10	5	-- Fail --	-- NA --	-- NA --	-- NA --	11.52
10	6	-- Fail --	-- NA --	-- NA --	-- NA --	18.56
10	7	-- Fail --	-- NA --	-- NA --	-- NA --	15.96
10	8	-- Fail --	-- NA --	-- NA --	-- NA --	19.88
10	9	-- Fail --	-- NA --	-- NA --	-- NA --	15.35
10	10	-- Fail --	-- NA --	-- NA --	-- NA --	27.3
10	11	-- Fail --	-- NA --	-- NA --	-- NA --	123.56
Mapped Lane Length:						283.46
11	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
11	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	0.46
11	2	-- Pass --	-- Fail --	-- Fail --	-- Fail --	25.81
11	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	12.18
11	4	-- Fail --	-- NA --	-- NA --	-- NA --	8.91
11	5	-- Fail --	-- NA --	-- NA --	-- NA --	10.78
11	6	-- Fail --	-- NA --	-- NA --	-- NA --	12.22
11	7	-- Fail --	-- NA --	-- NA --	-- NA --	13.96
11	8	-- Fail --	-- NA --	-- NA --	-- NA --	13.5
11	9	-- Fail --	-- NA --	-- NA --	-- NA --	13.75
Mapped Lane Length:						111.57
12	0	-- Pass --	-- Fail --	-- Fail --	-- NA --	0
12	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	18.84
12	2	-- Fail --	-- NA --	-- NA --	-- NA --	60.77
12	3	-- Pass --	-- Fail --	-- Fail --	-- Fail --	43.57
12	4	-- Fail --	-- NA --	-- NA --	-- NA --	9.02
12	5	-- Fail --	-- NA --	-- NA --	-- NA --	8.77
Mapped Lane Length:						140.97
13	0	-- Pass --	-- Fail --	-- Fail --	-- NA --	0

Appendix B: Increased Accuracy Thresholds

13	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	0.04
13	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	50.7
13	3	-- Fail --	-- NA --	-- NA --	-- NA --	82.71
13	4	-- Pass --	-- Fail --	-- Fail --	-- NA --	19.28
13	5	-- Fail --	-- NA --	-- NA --	-- NA --	24.9
13	6	-- Fail --	-- NA --	-- NA --	-- NA --	72.05
Mapped Lane Length:						249.68
14	0	-- Pass --	-- Fail --	-- Fail --	-- NA --	0
14	1	-- Fail --	-- NA --	-- NA --	-- NA --	31.39
14	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	42.09
14	3	-- Fail --	-- NA --	-- NA --	-- NA --	48.33
14	4	-- Fail --	-- NA --	-- NA --	-- NA --	50.11
14	5	-- Fail --	-- NA --	-- NA --	-- NA --	77.08
Mapped Lane Length:						249
15	0	-- Pass --	-- Fail --	-- Fail --	-- NA --	0
15	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	24.17
15	2	-- Fail --	-- NA --	-- NA --	-- NA --	52.78
15	3	-- Fail --	-- NA --	-- NA --	-- Fail --	59
15	4	-- Fail --	-- NA --	-- NA --	-- NA --	28.89
Mapped Lane Length:						164.84
Pass		17				
Fail		90				

Plymouth Road and Huron Parkway ± 0.4 Meters

Table 7 - Analysis Report for Plymouth Road and Huron Parkway ± 0.4 Meters

<<< START of MAP ASSESSMENT REPORT >>>						
Ingress		Node Pos	Lane Width	Altitude	Node Dist	Distance
Lane Id	Node #	Accuracy	Accuracy	Accuracy	for Curve	Bet Node(m)
3	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
3	1	-- Fail --	-- NA --	-- NA --	-- NA --	11.01
3	2	-- Fail --	-- NA --	-- NA --	-- Fail --	34.19
3	3	-- Fail --	-- NA --	-- NA --	-- NA --	15.3
Mapped Lane Length:						60.5
4	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
4	1	-- Fail --	-- NA --	-- NA --	-- NA --	0.23
4	2	-- Fail --	-- NA --	-- NA --	-- NA --	16.9
4	3	-- Fail --	-- NA --	-- NA --	-- NA --	31.91
4	4	-- Fail --	-- NA --	-- NA --	-- NA --	23.36
4	5	-- Fail --	-- NA --	-- NA --	-- NA --	91.17
Mapped Lane Length:						163.57
5	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
5	1	-- Fail --	-- NA --	-- NA --	-- NA --	0.09
5	2	-- Fail --	-- NA --	-- NA --	-- NA --	9.7
5	3	-- Fail --	-- NA --	-- NA --	-- NA --	27.73
5	4	-- Fail --	-- NA --	-- NA --	-- NA --	44.83
5	5	-- Fail --	-- NA --	-- NA --	-- NA --	81.1
Mapped Lane Length:						163.45
6	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
6	1	-- Fail --	-- NA --	-- NA --	-- NA --	14.53
6	2	-- Fail --	-- NA --	-- NA --	-- NA --	24.5
6	3	-- Fail --	-- NA --	-- NA --	-- NA --	15.2
6	4	-- Fail --	-- NA --	-- NA --	-- NA --	13.96
Mapped Lane Length:						68.19
7	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
7	1	-- Fail --	-- NA --	-- NA --	-- NA --	20.26
7	2	-- Fail --	-- NA --	-- NA --	-- NA --	34.87
7	3	-- Fail --	-- NA --	-- NA --	-- NA --	28.07

Appendix B: Increased Accuracy Thresholds

7	4	-- Fail --	-- NA --	-- NA --	-- NA --	28.97
7	5	-- Fail --	-- NA --	-- NA --	-- NA --	23.04
7	6	-- Fail --	-- NA --	-- NA --	-- NA --	17.45
7	7	-- Fail --	-- NA --	-- NA --	-- NA --	15.95
7	8	-- Fail --	-- NA --	-- NA --	-- NA --	11.86
7	9	-- Fail --	-- NA --	-- NA --	-- NA --	12.74
7	10	-- Fail --	-- NA --	-- NA --	-- NA --	14.88
7	11	-- Fail --	-- NA --	-- NA --	-- NA --	17.97
7	12	-- Fail --	-- NA --	-- NA --	-- NA --	15.3
7	13	-- Fail --	-- NA --	-- NA --	-- NA --	18.79
7	14	-- Fail --	-- NA --	-- NA --	-- NA --	16.85
7	15	-- Fail --	-- NA --	-- NA --	-- NA --	20.57
7	16	-- Fail --	-- NA --	-- NA --	-- NA --	133.29
Mapped Lane Length:						430.86
8	0	-- Pass --	-- Fail --	-- Fail --	-- NA --	0
8	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	0.16
8	2	-- Fail --	-- NA --	-- NA --	-- NA --	15.39
8	3	-- Fail --	-- NA --	-- NA --	-- NA --	21.87
8	4	-- Fail --	-- NA --	-- NA --	-- NA --	41.37
8	5	-- Fail --	-- NA --	-- NA --	-- NA --	31.61
8	6	-- Fail --	-- NA --	-- NA --	-- NA --	37.82
8	7	-- Fail --	-- NA --	-- NA --	-- NA --	15.07
8	8	-- Fail --	-- NA --	-- NA --	-- NA --	14.78
8	9	-- Fail --	-- NA --	-- NA --	-- NA --	15.98
8	10	-- Fail --	-- NA --	-- NA --	-- NA --	12.21
8	11	-- Fail --	-- NA --	-- NA --	-- NA --	17.63
8	12	-- Fail --	-- NA --	-- NA --	-- NA --	18.03
8	13	-- Fail --	-- NA --	-- NA --	-- NA --	16.12
8	14	-- Fail --	-- NA --	-- NA --	-- NA --	36.66
8	15	-- Fail --	-- NA --	-- NA --	-- NA --	134.14
Mapped Lane Length:						428.84
9	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
9	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	0.12
9	2	-- Pass --	-- Fail --	-- Fail --	-- Fail --	18.09
9	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	13.04
9	4	-- Fail --	-- NA --	-- NA --	-- NA --	12.21
9	5	-- Fail --	-- NA --	-- NA --	-- NA --	10.93
9	6	-- Fail --	-- NA --	-- NA --	-- NA --	22.22

Mapped Lane Length:						76.61
10	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
10	1	-- Fail --	-- NA --	-- NA --	-- NA --	0.28
10	2	-- Pass --	-- Fail --	-- Fail --	-- Fail --	24.62
10	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	14.25
10	4	-- Fail --	-- NA --	-- NA --	-- NA --	12.18
10	5	-- Fail --	-- NA --	-- NA --	-- NA --	11.52
10	6	-- Fail --	-- NA --	-- NA --	-- NA --	18.56
10	7	-- Fail --	-- NA --	-- NA --	-- NA --	15.96
10	8	-- Fail --	-- NA --	-- NA --	-- NA --	19.88
10	9	-- Fail --	-- NA --	-- NA --	-- NA --	15.35
10	10	-- Fail --	-- NA --	-- NA --	-- NA --	27.3
10	11	-- Fail --	-- NA --	-- NA --	-- NA --	123.56
Mapped Lane Length:						283.46
11	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
11	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	0.46
11	2	-- Pass --	-- Fail --	-- Fail --	-- Fail --	25.81
11	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	12.18
11	4	-- Fail --	-- NA --	-- NA --	-- NA --	8.91
11	5	-- Fail --	-- NA --	-- NA --	-- NA --	10.78
11	6	-- Fail --	-- NA --	-- NA --	-- NA --	12.22
11	7	-- Fail --	-- NA --	-- NA --	-- NA --	13.96
11	8	-- Fail --	-- NA --	-- NA --	-- NA --	13.5
11	9	-- Fail --	-- NA --	-- NA --	-- NA --	13.75
Mapped Lane Length:						111.57
12	0	-- Pass --	-- Fail --	-- Fail --	-- NA --	0
12	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	18.84
12	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	60.77
12	3	-- Pass --	-- Fail --	-- Fail --	-- Fail --	43.57
12	4	-- Fail --	-- NA --	-- NA --	-- NA --	9.02
12	5	-- Fail --	-- NA --	-- NA --	-- NA --	8.77
Mapped Lane Length:						140.97
13	0	-- Pass --	-- Fail --	-- Fail --	-- NA --	0
13	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	0.04
13	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	50.7
13	3	-- Fail --	-- NA --	-- NA --	-- NA --	82.71

Appendix B: Increased Accuracy Thresholds

13	4	-- Pass --	-- Fail --	-- Fail --	-- NA --	19.28
13	5	-- Fail --	-- NA --	-- NA --	-- NA --	24.9
13	6	-- Fail --	-- NA --	-- NA --	-- NA --	72.05
Mapped Lane Length:						249.68
14	0	-- Pass --	-- Fail --	-- Fail --	-- NA --	0
14	1	-- Fail --	-- NA --	-- NA --	-- NA --	31.39
14	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	42.09
14	3	-- Fail --	-- NA --	-- NA --	-- NA --	48.33
14	4	-- Fail --	-- NA --	-- NA --	-- NA --	50.11
14	5	-- Fail --	-- NA --	-- NA --	-- NA --	77.08
Mapped Lane Length:						249
15	0	-- Pass --	-- Fail --	-- Fail --	-- NA --	0
15	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	24.17
15	2	-- Fail --	-- NA --	-- NA --	-- NA --	52.78
15	3	-- Fail --	-- NA --	-- NA --	-- Fail --	59
15	4	-- Fail --	-- NA --	-- NA --	-- NA --	28.89
Mapped Lane Length:						164.84
Pass		22				
Fail		85				

Moravian Drive and Garfield Road ± 0.3 Meters

Table 8 - Accuracy Report for Moravian Drive and Garfield Road ± 0.3 Meters

<<< START of MAP ASSESSMENT REPORT >>>						
+/- 30cm						
Ingress	Node Pos	Lane Width	Altitude	Node Dist	Distance	
Lane Id	Node #	Accuracy	Accuracy	Accuracy	for Curve	Bet Node(m)
1	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
1	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	94.86
1	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	33.03
1	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	5.91
1	4	-- Pass --	-- Fail --	-- Fail --	-- NA --	55.25
1	5	-- Pass --	-- Fail --	-- Fail --	-- NA --	5.74
1	6	-- Pass --	-- NA --	-- Fail --	-- NA --	39.65
1	7	-- Fail --	-- NA --	-- NA --	-- NA --	36.41
Mapped Lane Length:						270.85
2	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
2	1	-- Fail --	-- NA --	-- NA --	-- NA --	269.91
Mapped Lane Length:						269.91
3	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
3	1	-- Fail --	-- NA --	-- NA --	-- Fail --	99.58
3	2	-- Fail --	-- NA --	-- NA --	-- NA --	29.54
Mapped Lane Length:						129.12
4	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
4	1	-- Fail --	-- NA --	-- NA --	-- Fail --	37.55
4	2	-- Fail --	-- NA --	-- NA --	-- NA --	7.63
Mapped Lane Length:						45.18
5	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
5	1	-- Fail --	-- NA --	-- NA --	-- NA --	4.07
5	2	-- Fail --	-- NA --	-- NA --	-- NA --	31.93
5	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	69.6
5	4	-- Pass --	-- Fail --	-- Fail --	-- NA --	67.12
5	5	-- Pass --	-- Fail --	-- Fail --	-- NA --	36.58
5	6	-- Pass --	-- Fail --	-- Fail --	-- NA --	66.88
Mapped Lane Length:						276.18

Appendix B: Increased Accuracy Thresholds

6	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
6	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	68.29
6	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	10.91
6	3	-- Fail --	-- NA --	-- NA --	-- NA --	26.63
Mapped Lane Length:						105.83
7	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
7	1	-- Fail --	-- NA --	-- NA --	-- NA --	38.04
7	2	-- Fail --	-- NA --	-- NA --	-- NA --	9.2
7	3	-- Fail --	-- NA --	-- NA --	-- NA --	8.78
Mapped Lane Length:						56.02
8	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
8	1	-- Fail --	-- NA --	-- NA --	-- NA --	42.6
8	2	-- Fail --	-- NA --	-- NA --	-- NA --	25.83
8	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	30.4
8	4	-- Fail --	-- NA --	-- NA --	-- NA --	182.77
Mapped Lane Length:						281.6
9	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
9	1	-- Fail --	-- NA --	-- NA --	-- NA --	280.55
Mapped Lane Length:						280.55
10	0	-- Pass --	-- Fail --	-- Fail --	-- NA --	0
10	1	-- Pass --	-- Fail --	-- Fail --	-- Fail --	71.92
10	2	-- Fail --	-- NA --	-- NA --	-- NA --	9.12
10	3	-- Fail --	-- NA --	-- NA --	-- NA --	18.98
Mapped Lane Length:						100.02
11	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
11	1	-- Fail --	-- NA --	-- NA --	-- Fail --	37.44
11	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	3.25
11	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	1.48
11	4	-- Fail --	-- NA --	-- NA --	-- NA --	6.98
Mapped Lane Length:						49.15
12	0	-- Pass --	-- Fail --	-- Fail --	-- NA --	0
12	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	33.53
12	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	22.47
12	3	-- Fail --	-- NA --	-- NA --	-- NA --	11.61

12	4	-- Fail --	-- NA --	-- NA --	-- NA --	10.38
12	5	-- Fail --	-- NA --	-- NA --	-- NA --	6.72
12	6	-- Fail --	-- NA --	-- NA --	-- NA --	9.37
12	7	-- Fail --	-- NA --	-- NA --	-- NA --	6.78
12	8	-- Fail --	-- NA --	-- NA --	-- NA --	5.27
12	9	-- Fail --	-- NA --	-- NA --	-- NA --	7.71
12	10	-- Fail --	-- NA --	-- NA --	-- NA --	13.76
12	11	-- Fail --	-- NA --	-- NA --	-- NA --	14.11
12	12	-- Fail --	-- NA --	-- NA --	-- NA --	61.3
12	13	-- Pass --	-- Fail --	-- Fail --	-- NA --	55.98
Mapped Lane Length:						258.99
13	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
13	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	56.22
13	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	7.11
13	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	13.2
13	4	-- Fail --	-- NA --	-- NA --	-- NA --	26.16
Mapped Lane Length:						102.69
14	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
14	1	-- Pass --	-- Fail --	-- Fail --	-- Fail --	39.28
14	2	-- Fail --	-- NA --	-- NA --	-- NA --	11.4
Mapped Lane Length:						50.68
Pass		25				
Fail		44				

Moravian Drive and Garfield Road ± 0.4 Meters

Table 9 - Accuracy Report for Moravian Drive and Garfield Road ± 0.4 Meters

<<< START of MAP ASSESSMENT REPORT >>>						
+/- 40cm						
Ingress	Node Pos	Lane Width	Altitude	Node Dist	Distance	
Lane Id	Node #	Accuracy	Accuracy	Accuracy	for Curve	Bet Node(m)
1	0	-- Pass --	-- Fail --	-- Fail --	-- NA --	0
1	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	94.86
1	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	33.03
1	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	5.91
1	4	-- Pass --	-- Fail --	-- Fail --	-- NA --	55.25
1	5	-- Pass --	-- Fail --	-- Fail --	-- NA --	5.74
1	6	-- Pass --	-- NA --	-- Fail --	-- NA --	39.65
1	7	-- Fail --	-- NA --	-- NA --	-- NA --	36.41
Mapped Lane Length:						270.85
2	0	-- Pass --	-- Fail --	-- Fail --	-- NA --	0
2	1	-- Fail --	-- NA --	-- NA --	-- NA --	269.91
Mapped Lane Length:						269.91
3	0	-- Pass --	-- Fail --	-- Fail --	-- NA --	0
3	1	-- Pass --	-- Fail --	-- Fail --	-- Fail --	99.58
3	2	-- Fail --	-- NA --	-- NA --	-- NA --	29.54
Mapped Lane Length:						129.12
4	0	-- Pass --	-- Fail --	-- Fail --	-- NA --	0
4	1	-- Fail --	-- NA --	-- NA --	-- Fail --	37.55
4	2	-- Fail --	-- NA --	-- NA --	-- NA --	7.63
Mapped Lane Length:						45.18
5	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
5	1	-- Fail --	-- NA --	-- NA --	-- NA --	4.07
5	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	31.93
5	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	69.6
5	4	-- Pass --	-- Fail --	-- Fail --	-- NA --	67.12
5	5	-- Pass --	-- Fail --	-- Fail --	-- NA --	36.58
5	6	-- Pass --	-- Fail --	-- Fail --	-- NA --	66.88
Mapped Lane Length:						276.18

Appendix B: Increased Accuracy Thresholds

6	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
6	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	68.29
6	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	10.91
6	3	-- Fail --	-- NA --	-- NA --	-- NA --	26.63
Mapped Lane Length:						105.83
7	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
7	1	-- Fail --	-- NA --	-- NA --	-- NA --	38.04
7	2	-- Fail --	-- NA --	-- NA --	-- NA --	9.2
7	3	-- Fail --	-- NA --	-- NA --	-- NA --	8.78
Mapped Lane Length:						56.02
8	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
8	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	42.6
8	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	25.83
8	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	30.4
8	4	-- Fail --	-- NA --	-- NA --	-- NA --	182.77
Mapped Lane Length:						281.6
9	0	-- Pass --	-- Fail --	-- Fail --	-- NA --	0
9	1	-- Fail --	-- NA --	-- NA --	-- NA --	280.55
Mapped Lane Length:						280.55
10	0	-- Pass --	-- Fail --	-- Fail --	-- NA --	0
10	1	-- Pass --	-- Fail --	-- Fail --	-- Fail --	71.92
10	2	-- Fail --	-- NA --	-- NA --	-- NA --	9.12
10	3	-- Fail --	-- NA --	-- NA --	-- NA --	18.98
Mapped Lane Length:						100.02
11	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
11	1	-- Pass --	-- Fail --	-- Fail --	-- Fail --	37.44
11	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	3.25
11	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	1.48
11	4	-- Fail --	-- NA --	-- NA --	-- NA --	6.98
Mapped Lane Length:						49.15
12	0	-- Pass --	-- Fail --	-- Fail --	-- NA --	0
12	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	33.53
12	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	22.47
12	3	-- Fail --	-- NA --	-- NA --	-- NA --	11.61

Appendix B: Increased Accuracy Thresholds

12	4	-- Pass --	-- Fail --	-- Fail --	-- NA --	10.38
12	5	-- Fail --	-- NA --	-- NA --	-- NA --	6.72
12	6	-- Fail --	-- NA --	-- NA --	-- NA --	9.37
12	7	-- Fail --	-- NA --	-- NA --	-- NA --	6.78
12	8	-- Fail --	-- NA --	-- NA --	-- NA --	5.27
12	9	-- Fail --	-- NA --	-- NA --	-- NA --	7.71
12	10	-- Fail --	-- NA --	-- NA --	-- NA --	13.76
12	11	-- Fail --	-- NA --	-- NA --	-- NA --	14.11
12	12	-- Pass --	-- Fail --	-- Fail --	-- NA --	61.3
12	13	-- Pass --	-- Fail --	-- Fail --	-- NA --	55.98
Mapped Lane Length:						258.99
13	0	-- Pass --	-- Fail --	-- Fail --	-- NA --	0
13	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	56.22
13	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	7.11
13	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	13.2
13	4	-- Fail --	-- NA --	-- NA --	-- NA --	26.16
Mapped Lane Length:						102.69
14	0	-- Pass --	-- Fail --	-- Fail --	-- NA --	0
14	1	-- Pass --	-- Fail --	-- Fail --	-- Fail --	39.28
14	2	-- Fail --	-- NA --	-- NA --	-- NA --	11.4
Mapped Lane Length:						50.68
Pass		39				
Fail		30				

Moravian Drive and Metropolitan Parkway ± 0.3 Meters

Table 10 - Accuracy Report for Moravian Drive and Metropolitan Parkway ± 0.3 Meters

<<< START of MAP ASSESSMENT REPORT >>>						
+/- 30cm						
Ingress	Node Pos	Lane Width	Altitude	Node Dist	Distance	
Lane Id	Node #	Accuracy	Accuracy	Accuracy	for Curve	Bet Node(m)
1	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
1	1	-- Fail --	-- NA --	-- NA --	-- NA --	111.24
1	2	-- Fail --	-- NA --	-- NA --	-- NA --	53.48
1	3	-- Fail --	-- NA --	-- NA --	-- NA --	52.57
1	4	-- Fail --	-- NA --	-- NA --	-- NA --	24.51
Mapped Lane Length:						241.8
2	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
2	1	-- Fail --	-- NA --	-- NA --	-- Fail --	65.21
2	2	-- Fail --	-- NA --	-- NA --	-- NA --	40.33
Mapped Lane Length:						105.55
3	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
3	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	181.28
3	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	75.26
Mapped Lane Length:						256.54
4	0	-- Pass --	-- Fail --	-- NA --	-- NA --	0
4	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	248.7
Mapped Lane Length:						248.7
5	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
5	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	253.56
Mapped Lane Length:						253.56
6	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
6	1	-- Pass --	-- Fail --	-- NA --	-- NA --	55.6
6	2	-- Fail --	-- NA --	-- NA --	-- NA --	61.76
6	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	27.82
6	4	-- Pass --	-- Fail --	-- Fail --	-- NA --	19.06
6	5	-- Fail --	-- NA --	-- NA --	-- NA --	7.28
6	6	-- Pass --	-- Fail --	-- Fail --	-- NA --	5.12
6	7	-- Pass --	-- Fail --	-- Fail --	-- NA --	9.5

Appendix B: Increased Accuracy Thresholds

6	8	-- Fail --	-- NA --	-- NA --	-- NA --	6.82
6	9	-- Pass --	-- Fail --	-- Fail --	-- NA --	12.3
6	10	-- Pass --	-- Fail --	-- Fail --	-- NA --	6.43
6	11	-- Pass --	-- Fail --	-- Fail --	-- NA --	5.67
6	12	-- Pass --	-- Fail --	-- Fail --	-- NA --	10.02
6	13	-- Pass --	-- Fail --	-- Fail --	-- NA --	7.75
6	14	-- Pass --	-- Fail --	-- Fail --	-- NA --	12.32
Mapped Lane Length:						247.44
7	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
7	1	-- Pass --	-- Fail --	-- NA --	-- NA --	69.14
7	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	26.24
7	3	-- Fail --	-- NA --	-- NA --	-- NA --	33.53
Mapped Lane Length:						128.91
8	0	-- Pass --	-- Fail --	-- NA --	-- NA --	0
8	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	260.97
Mapped Lane Length:						260.97
9	0	-- Pass --	-- Fail --	-- NA --	-- NA --	0
9	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	239.71
9	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	25.26
Mapped Lane Length:						264.97
10	0	-- Pass --	-- Fail --	-- NA --	-- NA --	0
10	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	243.3
10	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	25.43
Mapped Lane Length:						268.72
Pass		26				
Fail		16				

Moravian Drive and Metropolitan Parkway ± 0.4 Meters

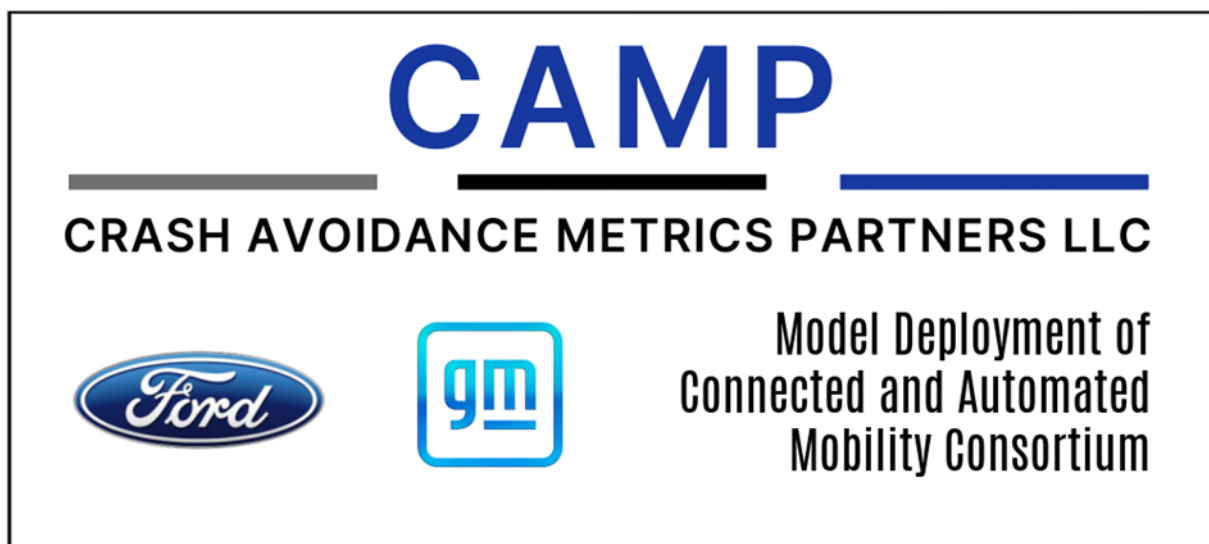
Table 11 - Accuracy Report for Moravian Drive and Metropolitan Parkway ± 0.4 Meters

<<< START of MAP ASSESSMENT REPORT >>>						
Ingress	Node Pos	Lane Width	Altitude	Node Dist	Distance	
Lane Id	Node #	Accuracy	Accuracy	Accuracy	for Curve	Bet Node(m)
1	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
1	1	-- Fail --	-- NA --	-- NA --	-- NA --	111.24
1	2	-- Fail --	-- NA --	-- NA --	-- NA --	53.48
1	3	-- Fail --	-- NA --	-- NA --	-- NA --	52.57
1	4	-- Fail --	-- NA --	-- NA --	-- NA --	24.51
				Mapped Lane Length:		241.8
2	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
2	1	-- Fail --	-- NA --	-- NA --	-- Fail --	65.21
2	2	-- Fail --	-- NA --	-- NA --	-- NA --	40.33
				Mapped Lane Length:		105.54
3	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
3	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	181.28
3	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	75.26
				Mapped Lane Length:		256.54
4	0	-- Pass --	-- Fail --	-- NA --	-- NA --	0
4	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	248.7
				Mapped Lane Length:		248.7
5	0	-- Pass --	-- Fail --	-- NA --	-- NA --	0
5	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	253.56
				Mapped Lane Length:		253.56
6	0	-- Fail --	-- NA --	-- NA --	-- NA --	0
6	1	-- Pass --	-- Fail --	-- NA --	-- NA --	55.6
6	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	61.76
6	3	-- Pass --	-- Fail --	-- Fail --	-- NA --	27.82
6	4	-- Pass --	-- Fail --	-- Fail --	-- NA --	19.06
6	5	-- Pass --	-- Fail --	-- Fail --	-- NA --	7.28
6	6	-- Pass --	-- Fail --	-- Fail --	-- NA --	5.12
6	7	-- Pass --	-- Fail --	-- Fail --	-- NA --	9.5

6	8	-- Pass --	-- Fail --	-- Fail --	-- NA --	6.82
6	9	-- Pass --	-- Fail --	-- Fail --	-- NA --	12.3
6	10	-- Pass --	-- Fail --	-- Fail --	-- NA --	6.43
6	11	-- Pass --	-- Fail --	-- Fail --	-- NA --	5.67
6	12	-- Pass --	-- Fail --	-- Fail --	-- NA --	10.02
6	13	-- Pass --	-- Fail --	-- Fail --	-- NA --	7.75
6	14	-- Pass --	-- Fail --	-- Fail --	-- NA --	12.32
Mapped Lane Length:						247.45
7	0	-- Pass --	-- Fail --	-- NA --	-- NA --	0
7	1	-- Pass --	-- Fail --	-- NA --	-- NA --	69.14
7	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	26.24
7	3	-- Fail --	-- NA --	-- NA --	-- NA --	33.53
Mapped Lane Length:						128.91
8	0	-- Pass --	-- Fail --	-- NA --	-- NA --	0
8	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	260.97
Mapped Lane Length:						260.97
9	0	-- Pass --	-- Fail --	-- NA --	-- NA --	0
9	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	239.71
9	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	25.26
Mapped Lane Length:						264.97
10	0	-- Pass --	-- Fail --	-- NA --	-- NA --	0
10	1	-- Pass --	-- Fail --	-- Fail --	-- NA --	243.3
10	2	-- Pass --	-- Fail --	-- Fail --	-- NA --	25.43
Mapped Lane Length:						268.73
Pass		31				
Fail		11				

Utah SMART Grant – Enabling Trust and Deployment Through Verified Connected Intersections Project

Validation Assessment & Analysis
Software Toolset User Guide
Version 3.0



Produced by Crash Avoidance Metrics Partners LLC in response to the United States Department of Transportation Project entitled “Enabling Trust and Deployment Through Verified Connected Intersections” under the SMART Grant program.

Report Documentation Page

Title and Subtitle Validation Assessment & Analysis Software Toolset User Guide	Report Date August 2025
Author(s) Parikh, J.	
Performing Organization Name and Address Crash Avoidance Metrics Partners LLC on behalf of the Model Deployment of Connected and Automated Mobility (MDCAM) Consortium 3050 Union Lake Rd., Unit 8F, 31 Commerce Township, MI 48382	Contract or Grant Utah SMART Grant – Enabling Trust and Deployment Through Verified Connected Intersections Project under the SMART Grant program.
Abstract This document serves as the user manual for a software toolset developed for the validation assessment and analysis of over-the-air SPaT and MAP broadcast messages for Connected Intersections. It is aimed at supporting the implementation of CIs that offer Red Light Violation Warning (RLVW). The toolset comprises several modules (software tools) that allow users to validate the transmission of Signal Phase and Timing (SPaT) in conjunction with the related MAP message.	
Key Words SPaT, MAP, software modules, toolset, Traffic Signal Controller, lane geometry	

Table of Contents

1	Introduction	1
1.1	System Requirements.....	3
1.1.1	Google Map API Key	3
1.2	Hierarchy of Toolset Software Modules.....	4
1.3	Validation Assessment and Analysis Software Toolset.....	4
2	SPaT and MAP Assessment Analysis	5
2.1.1	SPaT and MAP Assessment Analysis Graphical User Interface.....	5
3	SPaT Yellow Phase Assessment Analysis	11
3.1.1	Yellow Phase Assessment Analysis Graphical User Interface.....	11
4	MAP Validation Assessment and Analysis	16
4.1	MAP Validation Assessment	16
4.1.1	Software Tool – Graphical User Interface.....	16
5	References:	21
Appendix A	CI Performance Assessment Software Toolset.....	22

List of Figures

Figure 1: SPaT & MAP Verification Procedure	1
Figure 2: Verification and Validation Progression and Dependencies	2
Figure 3: Screenshot of GUI for SPaT and MAP Analysis	5
Figure 4: GUI Button Information and Process Execution Status Information.....	6
Figure 5: List of Separated Log Files by Intersection ID	7
Figure 6: SPaT Periodicity Plots Generated in SPaT Analysis Module	8
Figure 7: Visualization Screenshot of Intersection MAP and SPaT.....	9
Figure 8: Screenshot of GUI for SPaT Yellow Phase Analysis.....	11
Figure 9: Signal Phase Event Log Data Format.....	12
Figure 10: Example SPaT Yellow Phase Performance Analysis.....	13
Figure 11: Example SPaT Yellow Phase Performance Summary Report	14
Figure 12: Screenshot of YP Start Time and Duration Plots	14
Figure 13: Lane Boundary Mapping Data Processing.....	16
Figure 14: GUI for CI MAP Validation Assessment and Visualization.....	17
Figure 15: Example - User Information for File Selection	18
Figure 16: Example – MAP Validation Assessment Execution Progress	18
Figure 17: Example - Truncated MAP Validation Report.....	19
Figure 18: MAP Assessment Visualization Screenshot.....	20

List of Tables

Table 1: System Requirements for Software Toolset 3

Table 2: Toolset Software Module Hierarchy 22

List of Acronyms

ATSPM	Automated Traffic Signal Performance Measures
CAMP	Crash Avoidance Metrics Partners LLC
CI	Connected Intersection
CSV	Comma Separated Value
CTI	Connected Transportation Interoperability
GUI	Graphical User Interface
JSON	JavaScript Object Notation
MAP	Map of Intersection Geometry
PCAP	Packet Capture
PNG	Portable Network Graphics
RLVW	Red Light Violation Warning
SAE	SAE International
SPaT	Signal Phase and Timing
SPEL	Signal Phase Event Log
TSC	Traffic Signal Controller
UPER	Unaligned Packed Encoding Rules
V2I	Vehicle-to-Infrastructure
V2I-5	Vehicle-to-Infrastructure Consortium
YP	Yellow Phase

1 Introduction

This document serves as the user guide for a software toolset created for the Connected Intersection (CI) Program by the Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure 5 (V2I-5) Consortium (Ford, GM, and Nissan). This initiative was conducted to facilitate the deployment of CIs that provide Red Light Violation Warning (RLVW). Additionally, this guide has been updated under the Utah Department of Transportation SMART Grant – Enabling Trust and Deployment Through Verified Connected Intersections Project. The toolset contains multiple modules (software tools) that enable users to validate over-the-air transmission of Signal Phase and Timing (SPaT) along with the associated MAP messages.

In total, the toolset contains six software modules designed for verification and validation of SPaT and MAP to facilitate CI deployment for RLVW. Figure 1 illustrates the procedures associated in the verification and analysis of the recorded broadcast SPaT and MAP message.

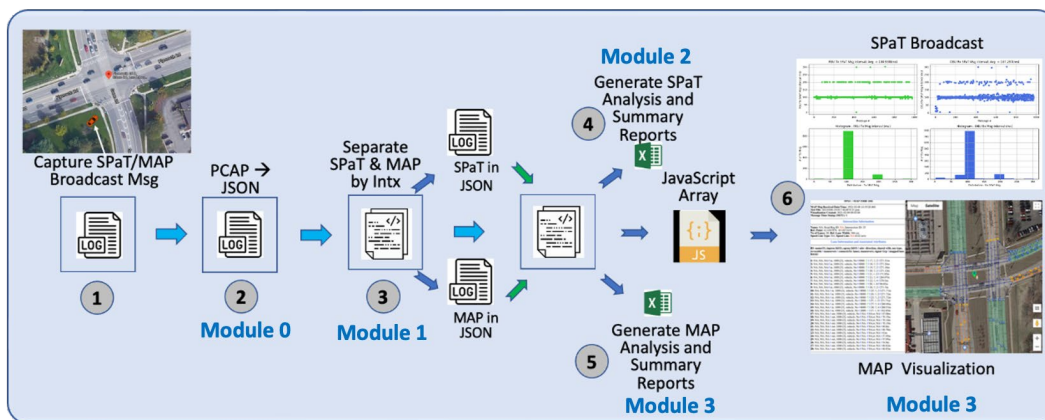


Figure 1: SPaT & MAP Verification Procedure

Modules 0 to 3 are described below.

- Module 0: Message Conversion – This module converts over the air binary broadcast messages (Packet Capture (PCAP) received in a log file in Unaligned Packet Encoding Rule (UPER) format to JavaScript Object Notation (JSON) for the next module in process.
- Module 1: Message Separation – This module selects SPaT and MAP messages in the JSON file and creates separate file for each based on intersection ID. The recorded PCAP file may include messages from multiple intersections that are within the range of the receiver that are also transmitting these messages.
- Module 2: SPaT Processing – This module analyzes the SPaT message file in JSON generated Module 1 for message conformity to SAE J2735 and CTI 4501 Guidance for

format, structure and required data elements for supporting RLVW. In addition, the following is generated in this module:

- SPaT message file in CSV
 - Conformity analysis pass/fail report for SPaT
 - Inter-message time interval plots for visual verification
- Module 3: MAP Processing – This module analyzes the MAP message file in JSON generated in the Module 1 for message conformity to SAE J2735 and CTI 4501 Guidance for format, structure and required data elements for supporting RLVW. In addition, the following is generated in this module:
 - MAP message file in CSV
 - Conformity analysis pass/fail report for MAP
 - Map geometry JavaScript data array for web browser-based visualization

Modules 4 and 5 make use of the output generated by Modules 2 and 3 for the validation assessment and additional analysis of the signal phase start time and duration, as well as for the validation assessment of the intersection lane geometry. Figure 2 depicts the progression and dependencies associated with Modules 4 and 5.

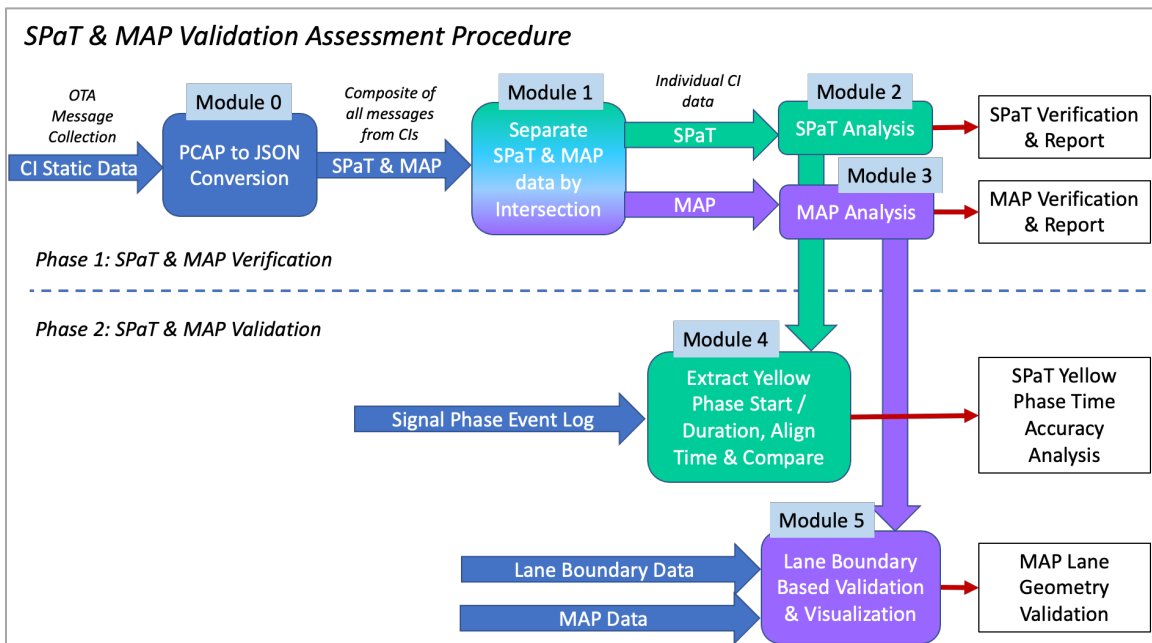


Figure 2: Verification and Validation Progression and Dependencies

Modules 4 and 5 are described below.

- Module 4: Yellow Phase analysis – This module evaluates the timing accuracy of the start of the yellow phase and its duration as set by the signal controller and the corresponding

processed SPaT messages (Module 2) for each activation across all signal groups. This module produces a collection of performance analyses for each signal group and summary reports.

- Module 5: MAP Lane Geometry Validation Assessment – This module processes the ingress lane boundary data that depicts the physical geometry of the lane for the computational determination of various lane attributes necessary for validation assessment and analysis of the lane geometry as defined in the MAP (Module 3).

1.1 System Requirements

The software modules for the toolset are developed using different programming languages to gain portability, provide inherent programming language efficiency, and to provide the capability for rapid prototyping and visualization. The machine operating the toolset must run a Windows operating system as well as the additional software packages listed in Table 1.

Table 1: System Requirements for Software Toolset

Software Package / Application S/W	Version	Function / Application
<ul style="list-style-type: none"> • Microsoft Windows 	<ul style="list-style-type: none"> • Version 10 or later 	<ul style="list-style-type: none"> • Target platform to run the software toolset
<ul style="list-style-type: none"> • Compiled source codes as .exe for MS Window • JavaScript 	<ul style="list-style-type: none"> • Windows version 10 or higher • Windows supported web browser 	<ul style="list-style-type: none"> • All six modules for processing and analysis • JavaScript for intersection MAP visualization for assessment in a web browser
<ul style="list-style-type: none"> • Google Map API Key 	<ul style="list-style-type: none"> • User is required to acquire a key https://developers.google.com/maps/documentation/javascript/get-api-key 	<ul style="list-style-type: none"> • A unique identifier key to access Google Map API in JavaScript used in visualizer <ul style="list-style-type: none"> ○ See Section 1.1.1 for the use of Google Map API Key
<ul style="list-style-type: none"> • Web Browser(s): MS Edge, Chrome, Firefox 	<ul style="list-style-type: none"> • Latest version 	<ul style="list-style-type: none"> • Connected Intersection MAP assessment visualization • Connected Intersection SPaT visualization

1.1.1 Google Map API Key

The MAP visualizer modules are based on Google Maps Platform products that use map API calls to display intersection maps and to render overlay information. The Google map products are secured from unauthorized use by restricting API calls to provide proper authentication credentials. These credentials are in the form of an API key, a unique alphanumeric string associates with the user's project.

A temporary Google MAP API key is included in the following files in source code for accessing google map for MAP visualization.

1. CI_SPaT+MAP_Analysis/CI_MAP+SPaT_Visualizer_v1b.html
2. CI_MAP_LB_Analysis/Visualizer/CI_MAP+LB_Visualizer_v3a.html

The user is required to acquire a new project Google Map API key and replace the existing temporary key in the above files with the new key for proper functioning of the visualizer modules. Visit: <https://developers.google.com/maps/documentation/javascript/get-api-key> website to acquire a key for more detail.

Replace **TEMPORARY KEY** with your key in the above two .html files.

```
<script async defer
  src =
    "https://maps.googleapis.com/maps/api/js?v=3&libraries=geometry&key=TEMPORARY
    KEY&callback=init_RLVW_map">
</script>
```

1.2 Hierarchy of Toolset Software Modules

The hierarchical list of the software modules used in the toolset along with the directory structure is provided in Appendix A in Table 2.

1.3 Validation Assessment and Analysis Software Toolset

The validation assessment and analysis toolset contains the following.

1. Validation assessment of broadcast SPaT and MAP messages for conformity with J2735[1] specification as well as requirements specified in ITE CTI 4501[2], CTI 4501/1[3] and CTI 4501/2[4] Connected Intersections Implementation Guides for SPaT and MAP Guidance
2. Comparative analysis of yellow phase start time and duration set by the signal controller with corresponding broadcast SPaT message for the same yellow phase for the signal group
3. Validation assessment of lane geometry of broadcast MAP message utilizing lane boundary data representing the physical lane geometry

2 SPaT and MAP Assessment Analysis

Modules 0, 1, 2, and 3 are integrated into a single executable application. The Graphical User Interface (GUI) for executing the three modules is illustrated in Figure 3. The application can be initiated either by executing the CI_SPaT+MAP_Analysis_GUI_v1b.exe from a command window within the application's installed directory or by directly launching it from the file explorer.

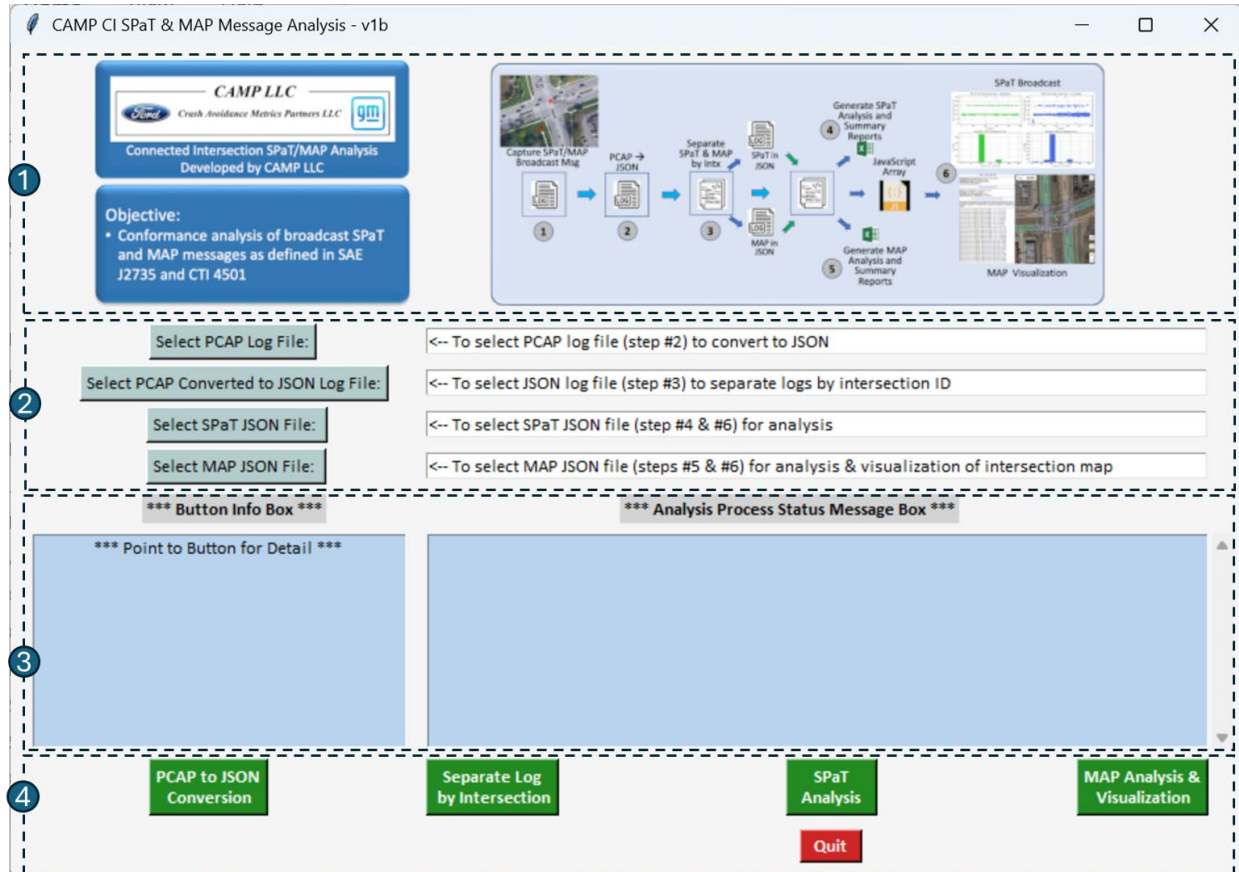


Figure 3: Screenshot of GUI for SPaT and MAP Analysis

2.1.1 SPaT and MAP Assessment Analysis Graphical User Interface

The GUI contains following four sections:

- Section 1: This section provides user the information about the modules in the tool and steps to analyze the recorded SPaT and MAP messages in PCAP.
- Section 2: This section provides buttons for user input of file selection. When a mouse pointer hovers over any button, the function associated with the input file is provided in

the Button Info Box. Also, the background color of the button is changed to indicate a selectable button.

- **Select PCAP Log File:** Click this button to select the recorded PCAP file to convert to JSON before launching the PCAP to JSON conversion (see Section 4). It is required that the recorded PCAP data is converted to JSON for subsequent processing steps.
 - **Select PCAP Converted to JSON Log File:** Click this button to select the file converted to JSON for separating SPaT and MAP logs by intersection ID. The recorded PCAP file may contain data from multiple CIs that are in proximity to the data recorder. It is required that all SPaT and MAP messages converted to JSON be separated by intersection ID.
 - **Select SPaT JSON File:** Click this button to select a SPaT file in JSON for the assessment and analysis of desired intersection.
 - **Select MAP JSON File:** Click this button to select a MAP file in JSON for the assessment and analysis as well as the web-based visualization of MAP. It is important that the selected SPaT and MAP files are for the same intersection.
- **Section 3:** This section provides two information boxes for the user. The relevant information about the functionality of the user input buttons (Section 2) and assessment analysis execution buttons in green (Section 4) are displayed in the Button Info Box when the mouse pointer hovers over it. The status information on the analysis process step being executed is displayed in the Analysis Process Status Message Box.

As an example, when the **SPaT Analysis** button is clicked, the Button Info Box displays the functionality associated with the button and the Analysis Process Status Message Box displays the progress status of the execution of the analysis. Figure 4 shows the screenshot of selected GUI button information and process execution status for the SPaT analysis.

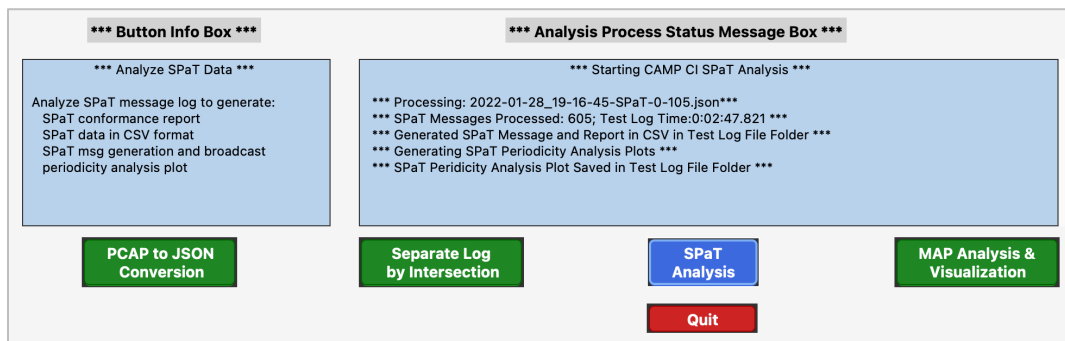


Figure 4: GUI Button Information and Process Execution Status Information

- Section 4: This section provides buttons to execute different steps in the analysis. When the specific step is executed, the background color of the button turns to Royal Blue. Use the following buttons to launch the desired processing and analysis functions.
 - **PCAP to JSON Conversion** Click this button to convert the recorded PCAP file to JSON file. It launches an external software module in a command window for the conversion. The progress of conversion will be shown on the command window.
 - **Separate Log by Intersection** Click this button to separate the composite JSON file of SPaT and MAP messages created in the previous step by intersection ID. The separated log files are stored in a separate subfolder by intersection ID in the test file folder. This creates a text file containing a list of intersection IDs. This file is stored in the same folder as the input file is shown in Figure 5.

```

*** Connected Intersection Field Test Verification ***

Input File: /Users/jsp-c/myStuff/MobilTel/CAMP (CIP+FHWA)/SPaT+MAP Verification/Veh_Test_Data/
TOSCo Test/PCAP-Jan-28-2022/2022-01-28_19-16-45/2022-01-28_19-16-45.json

Date & Time: 2023-05-02 09:02:40

Extracted SPaT File(s) for the Following 6 Intersection ID(s):
[0-102, 0-103, 0-104, 0-105, 0-106, 0-107]

>>> Missing SPaT Files for Intersection ID(s):{0-101} <<<

Following SPaT File(s) Created for Intersection ID(s):
2022-01-28_19-16-45-SPaT-0-102.json
2022-01-28_19-16-45-SPaT-0-103.json
2022-01-28_19-16-45-SPaT-0-104.json
2022-01-28_19-16-45-SPaT-0-105.json
2022-01-28_19-16-45-SPaT-0-106.json
2022-01-28_19-16-45-SPaT-0-107.json

Extracted MAP File(s) for the Following 7 Intersection ID(s):
[0-101, 0-102, 0-103, 0-104, 0-105, 0-106, 0-107]

Following MAP File(s) Created for Intersection ID(s):
2022-01-28_19-16-45-MAP-0-101.json
2022-01-28_19-16-45-MAP-0-102.json
2022-01-28_19-16-45-MAP-0-103.json
2022-01-28_19-16-45-MAP-0-104.json
2022-01-28_19-16-45-MAP-0-105.json
2022-01-28_19-16-45-MAP-0-106.json
2022-01-28_19-16-45-MAP-0-107.json

***** Not all Intersections have corresponding SPaT and MAP data files *****

```

Figure 5: List of Separated Log Files by Intersection ID

- **SPaT Analysis** Click this button for assessment and analysis of recorded SPaT messages. The following files are generated in this step.
 1. SPaT analysis summary report of message conformity as per J2735 and CTI 4501 for RLVW in CSV
 2. Processed SPaT messages in CSV for future analysis
 3. SPaT inter message generation and broadcast periodicity plots. An example is shown in Figure 6.
 4. Appropriate data array is built and stored in a file for visualization

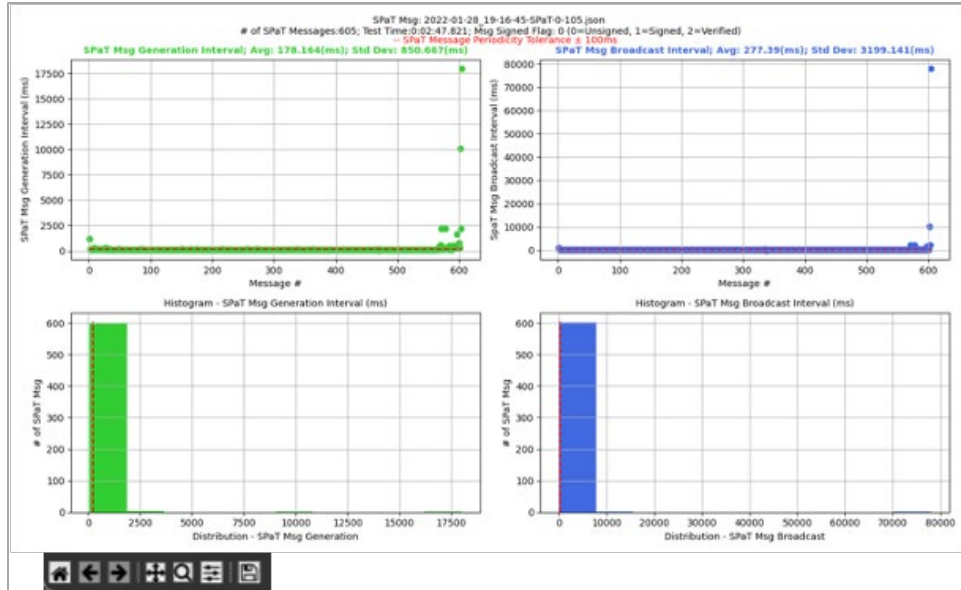



Figure 6: SPaT Periodicity Plots Generated in SPaT Analysis Module

The generated files are stored in the same directory as the input log data file by the intersection ID.

- **MAP Analysis & Visualization** Click this button to analyze and visualize the processed MAP message. The analysis generates the MAP conformity report, MAP data in CSV, builds appropriate data array and generates MAP visualization by over laying MAP data on the Google satellite view of the physical intersection in a web browser. The visualization provides animation of the associated SPaT status for each signal group from the processed SPaT message data generated in SPaT assessment analysis step. Figure 7 shows a screenshot of the intersection MAP and associated SPaT status for each signal group. Reports and plots are stored in the same folder as the log file.

For the MAP message, the web browser-based visualization provides full detail of the intersection lane definition with the associated node point attributes provided in the MAP message. Figure 7 shows MAP message detail in the panel on left. The geometric overlay of lane definitions is shown on the Google satellite view geometry of the intersection. The MAP reference point is marked as . The ingress lanes are shaded in light green and the node points defining the lane geometry are indicated by the blue circle with the lane id number. The egress lanes are indicated by orange-red lines with a directional arrow. The ingress lanes that connect to the corresponding egress lanes are indicated by a blue line with arrow indicating direction of egress. The Reference Point and each lane node points are clickable hotspots to see the absolute latitude, longitude of the point and other relevant information of the lane.

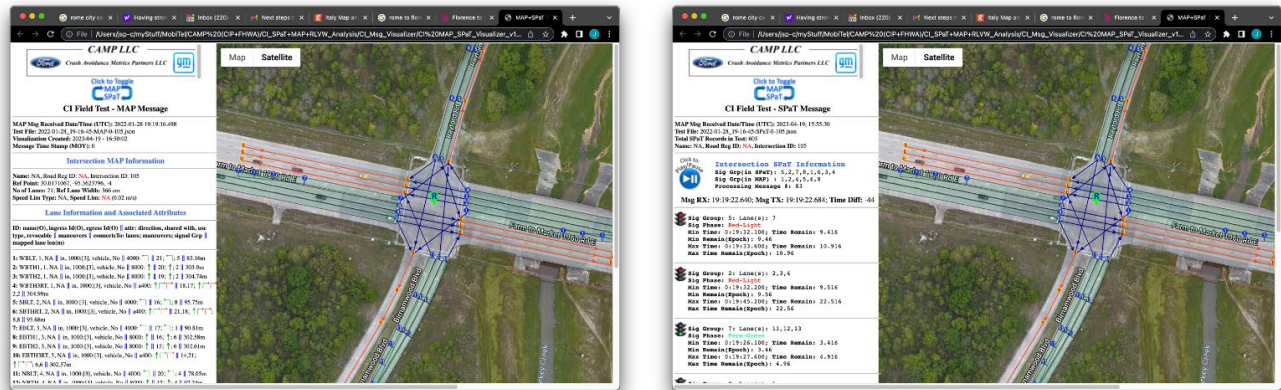



Figure 7: Visualization Screenshot of Intersection MAP and SPaT

As shown in Figure 7, the icon  provides the user a toggle between the MAP and SPaT message detail information in the panel. The SPaT information panel shows the following information for the intersection.




Intersection SPaT Information

Sig Grp(in SPaT): 5, 2, 7, 8, 1, 6, 3, 4

Sig Grp(in MAP): 1, 2, 4, 5, 6, 8

Processing Message #: 27

Msg RX: 19:19:16.767; **Msg Gen:** 19:19:16.795; **Time Diff:** -28

The total number of signal groups in SPaT and in MAP message is shown. For the current Message #27, the broadcast message received and the message generation timestamps along with the time difference between the two are shown in milliseconds (ms). The negative time difference (received time stamp is earlier than the message generation time) may indicate the internal clock of the message generating device is not synchronized with the same time source as a message receiving device. The clickable play/pause control icon  button enables the user to play and pause/resume of SPaT information for all signal groups in the message. The information is updated at every 100 milliseconds as the nominal SPaT update. As an example, the following information for each signal group is displayed.



Sig Group: 5: Lane(s): 7


Sig Phase: Red-Light

Min Time: 0:19:32.100; **Time Remain:** 15.914

Min Remain(Epoch): 15.945

Max Time: 0:20:02.100; **Time Remain:** 45.914

Max Time Remain(Epoch): 45.945

-  Click this button to end the SPaT and MAP assessment analysis toolset.

For more details on the functionality of the SPaT and MAP analysis, refer to CTI 4502v01.00 Connected Transportation Interoperability (CTI) Connected Intersections Validation Report [5].

3 SPaT Yellow Phase Assessment Analysis

Module 4, which performs yellow phase assessment analysis for basic RLW application, is described below.

3.1.1 Yellow Phase Assessment Analysis Graphical User Interface

The GUI for the Yellow Phase (YP) assessment analysis is shown in Figure 8. On a windows platform, it can be launched by either running the RLW_YP_Analysis_GUI_v2b.exe from a command window from the installed directory or by launching it directly from the file explorer.

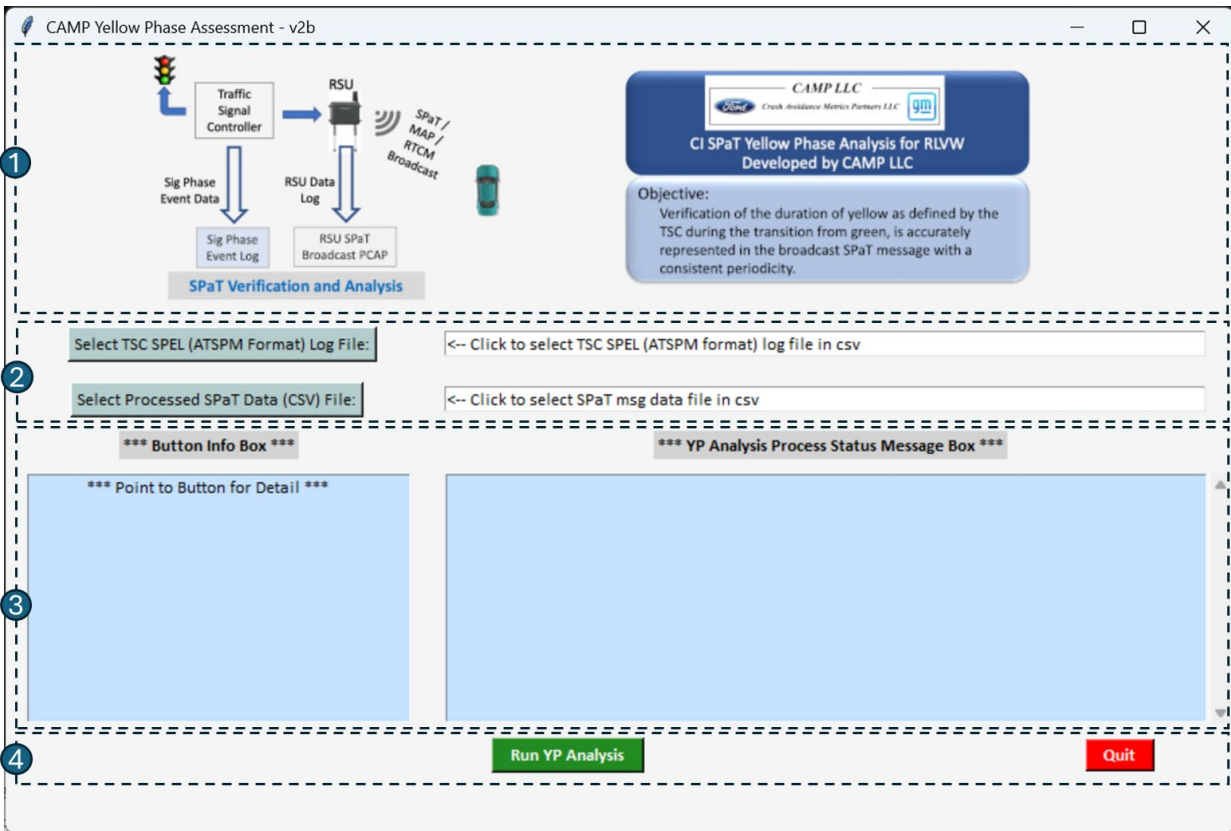



Figure 8: Screenshot of GUI for SPaT Yellow Phase Analysis

The GUI is divided into the following four sections similar to the other application GUIs described earlier.

- Section 1: This section illustrates information about the YP analysis tool for the recorded signal controller signal phase events and the processed broadcast SPaT messages described in Chapter 2.
- Section 2: This section provides buttons for input file selections. When a mouse pointer hovers over a button, information associated for file selection is displayed in the “***

Button Info Box ***.” At this point, the button’s background color is changed to indicate the user file selection button.

-  Click this button to select Traffic Signal Controller (TSC) signal phase state data transformed to Signal Phase Event Log (SPEL) in CSV. The existing implementation of SPEL utilizes the event code enumeration derived from the Automated Traffic Signal Performance Measures (ATSPM) by the data logger software. In the current implementation, the software supports controller log data and format are shown in Figure 9.

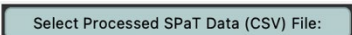

Signal Id	UTC Timestamp	Event Code	Event Parameter
7710	2024-10-02T14:47:03.557+0000	7	4
7710	2024-10-02T14:47:03.557+0000	8	4
7710	2024-10-02T14:47:06.861+0000	9	4
7710	2024-10-02T14:47:06.861+0000	10	4
7710	2024-10-02T14:47:06.861+0000	12	4
7710	2024-10-02T14:47:09.356+0000	0	2
7710	2024-10-02T14:47:09.356+0000	1	2
7710	2024-10-02T14:47:09.356+0000	0	6
7710	2024-10-02T14:47:09.356+0000	1	6
7710	2024-10-02T14:47:46.656+0000	7	2
7710	2024-10-02T14:47:46.656+0000	8	2
7710	2024-10-02T14:47:51.156+0000	9	2
7710	2024-10-02T14:47:51.156+0000	10	2
7710	2024-10-02T14:47:51.156+0000	12	2
7710	2024-10-02T14:47:53.156+0000	0	1
7710	2024-10-02T14:47:53.156+0000	1	1
7710	2024-10-02T14:48:13.657+0000	7	1
7710	2024-10-02T14:48:13.657+0000	8	1

Where:

- Signal ID: Intersection ID
- UTC Timestamp: yyyy-mm-ddThh:mm:ss.sss±hh
 - Date: year-month-day
 - T: follows time
 - Time: hour:minute:second.milliseconds±hour offset
 - Event Code: Signal Phase Event†
 - Event Param: Signal group# (1–255)†
 - File Format: Comma Separated Value

† For detail, see “Indiana Traffic Signal Hi Resolution Data Logger Enumerations”, August 2020 for detail at: <https://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1003&context=itrddata>

Figure 9: Signal Phase Event Log Data Format

-  Click this button to select the processed broadcast SPaT messages file generated in CSV as described in Chapter 2. The information from this file is used for comparing YP start time and the duration with the SPEL file generated by the data logger for the CI under assessment for analysis.
- Section 3: This section provides two information boxes for the user as described in Section 3.1.1 for relevant information about the functionality of the user input buttons (Section 2) and the “Run YP Analysis” button in green (Section 4) in the Button Info Box when the mouse pointer hovers over it. The status information on the analysis process being executed is displayed in the YP Analysis Process Status Message Box.
- Section 4: In this section,  button allows the user to run the YP analysis and to quit the tool. YP analysis generates the following:
 1. A detailed YP performance analysis report in CSV for all signal groups and for each event of YP start time and duration within the signal group. An example truncated report of following sets of analysis is shown in Figure 10.
 - a. TSC generated YP start time and duration
 - b. Corresponding YP start time and duration in the broadcast SPaT message
 - c. Time difference between the two

TSC Log: ATSPM				*** CI - TSC & SPaT Msg Yellow Phase Start and Duration Log ***										Col R = Col P + Col Q (ms)			
TSC Log File: 7706-atspm.csv				Log Created: 2024-10-22 08:41:26										Col S = Col M - Col F (ms)			
SPaT File: 7706-ota-SPaT-0-7706.csv				Intersection ID: 7706										Col T = Col N - Col F (ms)			
>>>> ===== Traffic Signal Controller Data =====<<<<<<				>>>> ===== SPaT Message Data =====<<<<<<										>>>> ===== YP Performance Time Diff =====<<<<<<			
SigGrp# 1	<----- Start Time ----->		<----- End Time ----->	Duration (sec)	<---- Msg Timestamp ---->	<- MsgRX Timestamp ->	Sig Indicator	Dur (minET) (sec)	Dur (MsgRX) (sec)	MsgTS & TSC Start (ms)	MsgRX & MsgTS (ms)	End-to-End TSC to OBU (ms)	<--- YP Dur Time Diff(s)--->	TSC & Msg (ms)	TSC & MsgRX (ms)		
	1	2024-10-12 01:38:07.735	2024-10-12 01:38:11.335	3.6	285d - 0:52:09.751	2024/10/12 00:52:09.780	Perm-Yellow	5.249	5.22	2757984	29	2758013	1649	1649	1620		
			TSC YP Duration Min:	3.6		SPaT YP Duration (Msg Gen / Msg Rcvd) Min:		5.249	5.22	Perf Min:	2757984	29	2758013	1649	1649		
			TSC YP Duration Max:	3.6		SPaT YP Duration (Msg Gen / Msg Rcvd) Max:		5.249	5.22	Perf Max:	2757984	29	2758013	1649	1649		
SigGrp# 2	1	2024-10-12 00:52:09.735	2024-10-12 00:52:15.139	5.404	285d - 0:52:09.751	2024/10/12 00:52:09.780	Prot-Yellow	5.249	5.22	16	29	45	155	184			
	2	2024-10-12 00:54:09.735	2024-10-12 00:54:15.139	5.404	285d - 0:54:09.751	2024/10/12 00:54:09.771	Prot-Yellow	5.249	5.229	16	20	36	155	175			
	3	2024-10-12 00:56:09.735	2024-10-12 00:56:15.139	5.404	285d - 0:56:09.751	2024/10/12 00:56:09.767	Prot-Yellow	5.249	5.233	16	16	32	155	171			
	4	2024-10-12 00:58:09.735	2024-10-12 00:58:15.139	5.404	285d - 0:58:09.751	2024/10/12 00:58:09.771	Prot-Yellow	5.249	5.229	16	20	36	155	175			
	5	2024-10-12 01:00:09.735	2024-10-12 01:00:15.139	5.404	285d - 1:00:09.750	2024/10/12 01:00:09.776	Prot-Yellow	5.25	5.224	15	26	41	154	180			
	6	2024-10-12 01:01:29.139	2024-10-12 01:01:34.535	5.396	285d - 1:01:29.150	2024/10/12 01:01:29.168	Prot-Yellow	5.25	5.232	11	18	29	146	164			
	7	2024-10-12 01:04:19.735	2024-10-12 01:04:25.139	5.404	285d - 1:04:19.751	2024/10/12 01:04:19.769	Prot-Yellow	5.249	5.231	16	18	34	155	173			
	8	2024-10-12 01:05:59.735	2024-10-12 01:06:05.139	5.404	285d - 1:05:59.751	2024/10/12 01:05:59.772	Prot-Yellow	5.249	5.228	16	21	37	155	176			
	9	2024-10-12 01:09:19.835	2024-10-12 01:09:25.235	5.4	285d - 1:09:19.851	2024/10/12 01:09:19.867	Prot-Yellow	39.849	39.833	16	16	32	34449	34433			
	10	2024-10-12 01:10:41.235	2024-10-12 01:10:46.635	5.4	285d - 1:10:41.251	2024/10/12 01:10:41.267	Prot-Yellow	5.249	5.233	16	16	32	151	167			
	11	2024-10-12 01:11:45.335	2024-10-12 01:11:50.735	5.4	285d - 1:11:45.352	2024/10/12 01:11:45.376	Prot-Yellow	5.248	5.224	17	24	41	152	176			
	12	2024-10-12 01:13:06.535	2024-10-12 01:13:11.935	5.4	285d - 1:13:06.551	2024/10/12 01:13:06.570	Prot-Yellow	5.249	5.23	16	19	35	151	170			
	13	2024-10-12 01:14:19.735	2024-10-12 01:14:25.139	5.404	285d - 1:14:19.751	2024/10/12 01:14:19.771	Prot-Yellow	5.249	5.229	16	20	36	155	175			
	14	2024-10-12 01:15:59.735	2024-10-12 01:16:05.139	5.404	285d - 1:15:59.751	2024/10/12 01:15:59.768	Prot-Yellow	5.249	5.232	16	17	33	155	172			
	15	2024-10-12 01:17:39.735	2024-10-12 01:17:45.139	5.404	285d - 1:17:39.751	2024/10/12 01:17:39.777	Prot-Yellow	5.249	5.223	16	26	42	155	181			
	16	2024-10-12 01:19:19.735	2024-10-12 01:19:25.139	5.404	285d - 1:19:19.750	2024/10/12 01:19:19.766	Prot-Yellow	5.25	5.234	15	16	31	154	170			
	17	2024-10-12 01:20:59.735	2024-10-12 01:21:05.139	5.404	285d - 1:20:59.751	2024/10/12 01:20:59.769	Prot-Yellow	5.249	5.231	16	18	34	155	173			
	18	2024-10-12 01:22:39.735	2024-10-12 01:22:45.139	5.404	285d - 1:22:39.751	2024/10/12 01:22:39.766	Prot-Yellow	5.249	5.234	16	15	31	155	170			
	19	2024-10-12 01:25:59.735	2024-10-12 01:26:05.139	5.404	285d - 1:25:59.751	2024/10/12 01:25:59.771	Prot-Yellow	5.249	5.229	16	20	36	155	175			
	20	2024-10-12 01:29:19.735	2024-10-12 01:29:25.139	5.404	285d - 1:29:19.751	2024/10/12 01:29:19.769	Prot-Yellow	5.249	5.231	16	18	34	155	173			
	21	2024-10-12 01:32:39.735	2024-10-12 01:32:45.139	5.404	285d - 1:32:39.751	2024/10/12 01:32:39.778	Prot-Yellow	5.249	5.222	16	27	43	155	182			
	22	2024-10-12 01:34:19.735	2024-10-12 01:34:25.139	5.404	285d - 1:34:19.751	2024/10/12 01:34:19.770	Prot-Yellow	5.249	5.23	16	19	35	155	174			
	23	2024-10-12 01:36:02.735	2024-10-12 01:36:08.139	5.404	285d - 1:36:02.752	2024/10/12 01:36:02.769	Prot-Yellow	5.248	5.231	17	17	34	156	173			
	24	2024-10-12 01:37:39.835	2024-10-12 01:37:45.235	5.4	285d - 1:37:39.851	2024/10/12 01:37:39.874	Prot-Yellow	39.849	39.826	16	23	39	34449	34426			
	25	2024-10-12 01:39:01.235	2024-10-12 01:39:06.635	5.4	285d - 1:39:01.251	2024/10/12 01:39:01.267	Prot-Yellow	5.249	5.233	16	16	32	151	167			
	26	2024-10-12 01:40:59.736	2024-10-12 01:41:05.139	5.403	285d - 1:40:59.751	2024/10/12 01:40:59.777	Prot-Yellow	5.249	5.223	15	26	41	154	180			
	27	2024-10-12 01:42:21.935	2024-10-12 01:42:27.335	5.4	285d - 1:42:21.952	2024/10/12 01:42:21.975	Prot-Yellow	39.848	39.825	17	23	40	34448	34425			
	28	2024-10-12 01:44:19.736	2024-10-12 01:44:25.139	5.403	285d - 1:44:19.751	2024/10/12 01:44:19.772	Prot-Yellow	5.249	5.228	15	21	36	154	175			
	29	2024-10-12 01:46:05.635	2024-10-12 01:46:11.041	5.406	285d - 1:46:05.651	2024/10/12 01:46:05.670	Prot-Yellow	5.249	5.23	16	19	35	157	176			
	30	2024-10-12 01:47:39.735	2024-10-12 01:47:45.139	5.404	285d - 1:47:39.751	2024/10/12 01:47:39.766	Prot-Yellow	5.249	5.234	16	15	31	155	170			
	31	2024-10-12 01:49:19.735	2024-10-12 01:49:25.139	5.404	285d - 1:49:19.751	2024/10/12 01:49:19.771	Prot-Yellow	5.249	5.229	16	20	36	155	175			
	32	2024-10-12 01:51:10.235	2024-10-12 01:51:15.635	5.4	285d - 1:51:10.251	2024/10/12 01:51:10.267	Prot-Yellow	5.249	5.233	16	16	32	151	167			
	33	2024-10-12 01:52:39.735	2024-10-12 01:52:45.139	5.404	285d - 1:52:39.750	2024/10/12 01:52:39.769	Prot-Yellow	5.25	5.231	15	19	34	154	173			
	34	2024-10-12 01:55:59.735	2024-10-12 01:56:05.139	5.404	285d - 1:55:59.751	2024/10/12 01:55:59.768	Prot-Yellow	5.249	5.232	16	17	33	155	172			
	35	2024-10-12 01:57:39.735	2024-10-12 01:57:45.139	5.404	285d - 1:57:39.751	2024/10/12 01:57:39.774	Prot-Yellow	5.249	5.226	16	23	39	155	178			
	36	2024-10-12 02:02:39.735	2024-10-12 02:02:45.139	5.404	285d - 2:02:39.754	2024/10/12 02:02:39.777	Prot-Yellow	5.246	5.223	19	23	42	158	181			
	37	2024-10-12 02:04:28.235	2024-10-12 02:04:33.635	5.4	285d - 2:04:28.251	2024/10/12 02:04:28.275	Prot-Yellow	5.249	5.225	16	24	40	151	175			
	38	2024-10-12 02:05:59.735	2024-10-12 02:06:05.139	5.404	285d - 2:05:59.751	2024/10/12 02:05:59.768	Prot-Yellow	5.249	5.232	16	17	33	155	172			
			TSC YP Duration Min:	5.396		SPaT YP Duration (Msg Gen / Msg Rcvd) Min:		5.246	5.22	Perf Min:	11	15	29	146	146		
			TSC YP Duration Max:	5.406		SPaT YP Duration (Msg Gen / Msg Rcvd) Max:		39.849	39.833	Perf Max:	19	29	45	34449	34449		

Figure 10: Example SPaT Yellow Phase Performance Analysis

2. A summary report of YP performance analysis in CSV indicating pass/fail based on the requirements in the CTI4501/1 SPaT Guidance is shown in Figure 11.

*** CI TSC & SPaT Message Yellow Phase Analysis Summary for RLWW - v0.5 ***				
Report Created: 2024-10-22; 08:41:26				
Intersection ID: 7706				
Test Name: SPaT - Test Location:				
TSC Log ATSPM				
TSC Log File: 7706-atspm.csv				
SPaT File: 7706-ota-SPaT-0-7706.csv				
# of SPaT Messages Processed: 44998				
<<<<< ===== YP Start Time Summary: TSC to SPaT Broadcast =====>>>>>				
		Time Diff(ms)	<-End-to-End: TSC to SPaT Broadcast ->	
Sig Grp #	SPaT v. TSC	Msg RX v. TSC	Pass / Fail	Remark
1	2757984	2758013	--Fail--	> 175ms
2	11	45	Pass	
3	--NA--	--NA--	--NA--	
4	10	45	Pass	
5	1047884	1047913	--Fail--	> 175ms
6	11	45	Pass	
7	--NA--	--NA--	--NA--	
8	10	45	Pass	
<<<<< ===== YP Duration Analysis Summary =====>>>>>				
		SPaT Msg minET(s)	Time Diff(s) SPaT vs. TSC	
Sig Grp #	TSC Time(s)			
1	3.6	5.249	1.649	
2	5.4	5.246	0.154	
3	--NA--	--NA--	--NA--	
4	3.6	3.445	0.155	
5	4.3	5.249	0.949	
6	5.4	5.246	0.154	
7	--NA--	--NA--	--NA--	
8	3.6	3.445	0.155	
8	3.6	3.445	0.155	
Notes:				
1. Yellow Phase Start Time Analysis Summary:				
a. Diff in start time (milliseconds) for the signal group - SPaT message vs. controller time				
b. End-to-end time difference (milliseconds) for the signal group - SPaT message received vs. the controller time				
c. --NA-- indicates absence of yellow phase in data for the signal group				
2. Yellow Phase Duration Analysis Summary:				
a. Reported YP duration - SPaT message and controller for the signal group				
b. Difference in duration - SPaT message and controller for the signal group				

Figure 11: Example SPaT Yellow Phase Performance Summary Report

3. In addition, the following two interactive analysis plots are shown in Figure 12:
 - a. Comparison plot of the start of yellow for each signal group as per the TSC and in the broadcast SPaT message
 - b. Corresponding comparison plot of the duration of yellow for each signal group as per the TSC and in the broadcast SPaT message

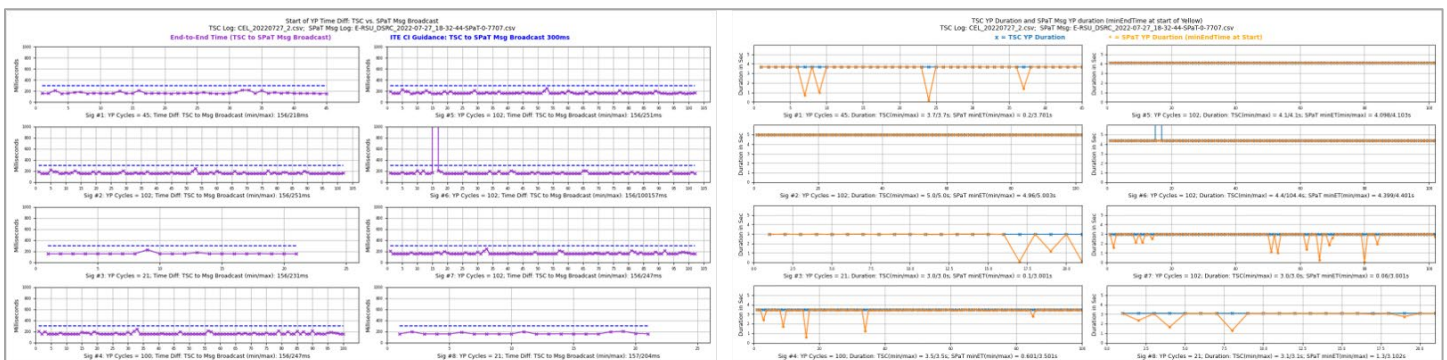


Figure 12: Screenshot of YP Start Time and Duration Plots

The generated report files in CVS and plot screenshot files in .png are stored in the same directory as the SPaT input file for the intersection under test.

4 MAP Validation Assessment and Analysis

This software tool offers validation assessment and analysis of the broadcast MAP message to ensure accuracy in accordance with the CTI4501/2 requirement regarding the geographic representation of the CI. The software tool utilizes lane boundary data produced through Mobile mapping data processing, and the lane boundary data is exported to CSV format for lane geometry validation. Figure 13 depicts the methodology employed to generate the data for processing, which is utilized by the software tool for MAP accuracy analysis.

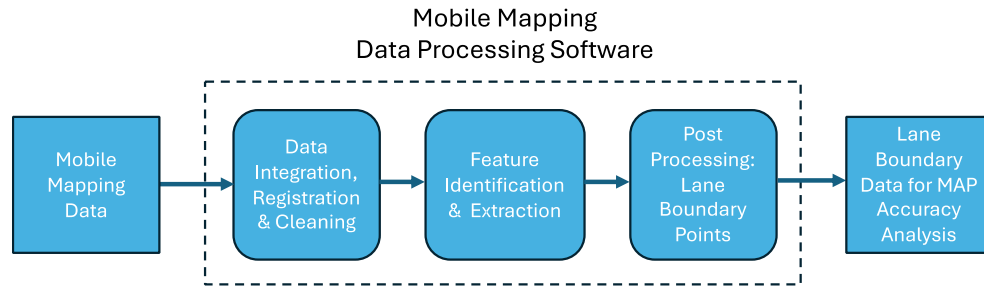


Figure 13: Lane Boundary Mapping Data Processing

4.1 MAP Validation Assessment

Module 5 offers validation assessment and visualization of the broadcast MAP message to ensure its accuracy as well as an assessment of the geographic representation of the CI. This module utilizes lane boundary data and the lane geometry defined in the broadcast MAP message for achieving the lane geometry node points validation. The following requirements of CTI 4501/2 are validated within this module of the toolset.

1. Positions of nodes for ingress lanes
 - a. The initial node point that establishes the stop point
 - b. Additional node points
2. Width of the lane at the node point
3. Elevation of the lane at the node point
4. Distance between node points along a curve
5. Overall length of the mapped lane

4.1.1 Software Tool – Graphical User Interface

The GUI for the MAP validation and analysis is shown in Figure 14. On a Windows platform, the CI_MAP_LB_Assessment_GUI_v3a.exe software can be launched by either:

- From the command prompt by navigating to the directory containing the .exe file along with its related files and subdirectories
- Accessed directly from the file folder within the file explorer

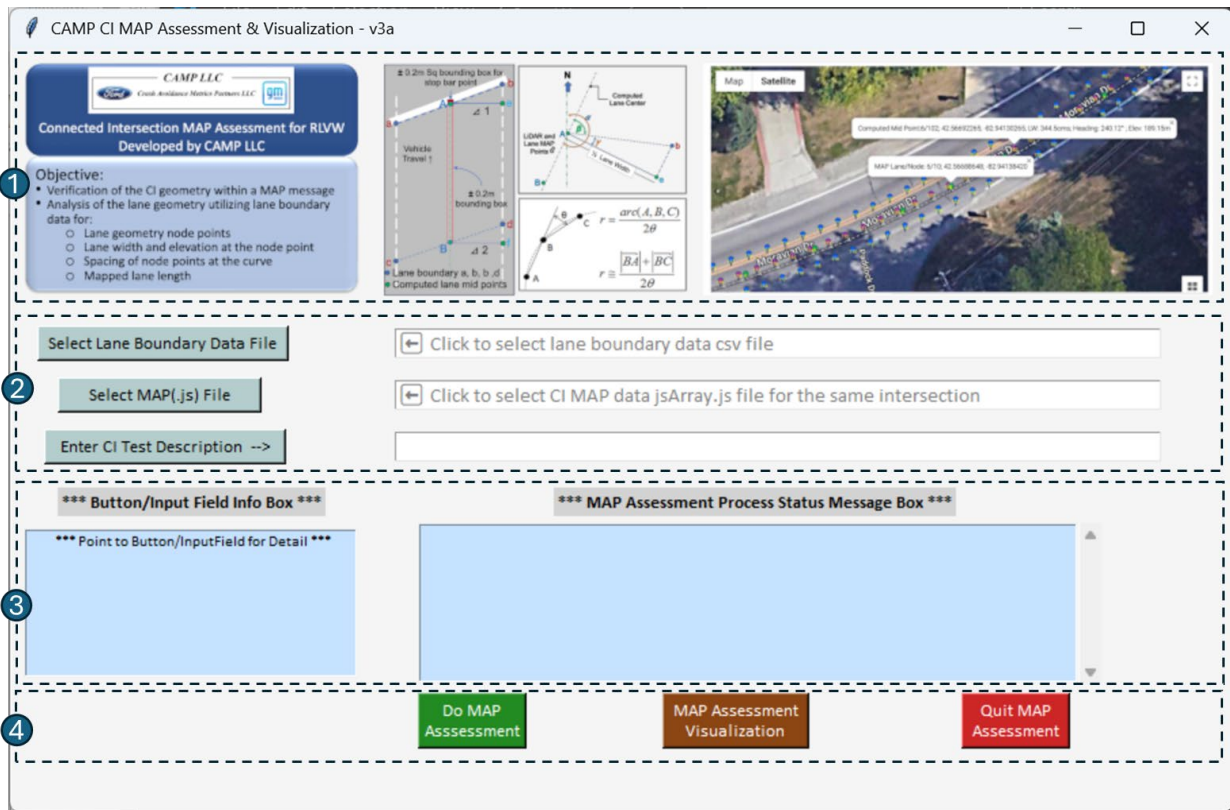


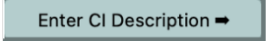

Figure 14: GUI for CI MAP Validation Assessment and Visualization

The MAP validation assessment and visualization toolset GUI is arranged in the following four sections.

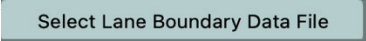
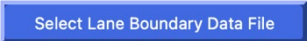
- Section 1: User Information – This section offers users details regarding the tool's purpose, the methodology employed for calculating physical lane geometry utilizing lane boundary data to ascertain lane center, lane width, and lane radius of curvature, as well as MAP visualization.
- Section 2: User input – In this section, the user interface for choosing input data files and providing input for the CI description is presented.

1. **Select Lane Boundary Data File** Select the lane boundary data file formatted in CSV for the CI validation assessment. Refer to the Utah Smart Grant - Enabling Trust and Deployment Through Verified Connected Intersections Project Assessing Node Point Accuracy and SAE J3238/2 "Verification of MAP Node Accuracy using Mobile Mapping Data at Connected Intersections to support in-vehicle Red Light Violation Warning" Report for the guidelines the CSV data file, which acts as the ground truth for the validation of the MAP.
2. **Select MAP(.js) File** Select previously generated MAP data arrays in JavaScript (.js) in Module 3. The processed MAP file contains map data arrays in JavaScript (...MAP_data_jsArray.js) for visualization. This file is located in folder

“Intersection_ID-0-xxxx” where xxxx indicates intersection ID. This input file is required to validate the broadcast MAP using the lane boundary data file for the MAP requirements and to generate data array file for visualization

3.   This input field allows user to enter description of the CI under assessment. The description is provided in the report generated by the tool.

- Section 3: In this section, two boxes for contextual information display to the user is provided.

- ***** Button / Input Field Info Box *****: In this information display box, relevant information about the functioning of the user input buttons with associated fields are provided. For instance, when the mouse hovers over the button or the  is selected, information about the input file selection is displayed as shown in Figure 15. In addition, the button background is changed to  indicate selection.

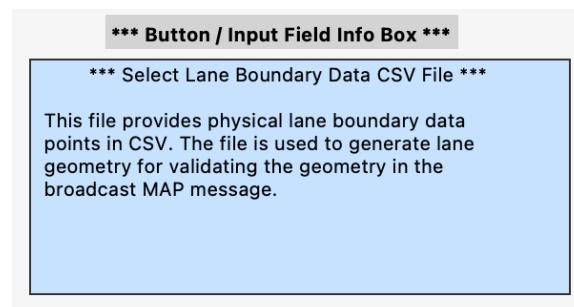


Figure 15: Example - User Information for File Selection

- ***** MAP Assessment/Visualization Process Status Message Box *****: This message box provides progress when user executes either the MAP assessment or MAP visualization. For instance, progress message is displayed in Figure 16 when the MAP validation assessment is being executed.

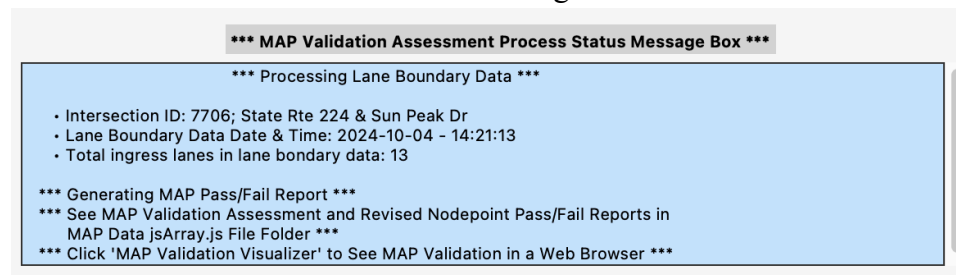
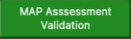




Figure 16: Example – MAP Validation Assessment Execution Progress

- Section 4: As illustrated in Figure 14, the following buttons are available for the validation assessment of MAP validation, for graphical visualization of MAP, and for exiting the tool.

1.  Click this button to initiate the MAP validation assessment. As detailed in Section 2 for the user input files, this procedure employs the lane boundary data (.csv) file in conjunction with the JavaScript (.js) file developed for the intersection in Module 3. This process generates a pass/fail report in CSV format. An example of truncated report file is illustrated in Figure 17. A data array file in JavaScript (.js) is also generated for use in the visualization.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S		
						*** Connected Intersection MAP Verification Test Report v2a.0 ***														
Description: UDOT Test Intersection																				
Lane Boundary Data File: /Users/jsp-c/myStuff/MobiTel/CAMP (CV PFS + SOADS + UDOT Smart Grant)/UDOT - Smart Grant/UDOT - MAP Assessment/UDOT Test/Intersection_ID-0-7706/7706.csv																				
Intersection Name: State Rte 224 & Sun Peak Dr																				
Intersection ID: 7706																				
LB Data File Date/Time: 2024-10-04 - 14:21:13																				
MAP File Date/Time: /Users/jsp-c/myStuff/MobiTel/CAMP (CV PFS + SOADS + UDOT Smart Grant)/UDOT - Smart Grant/UDOT - MAP Assessment/UDOT Test/Intersection_ID-0-7706/7706-ota-MAP-0-7706_MAP_data_jsArray.js																				
Process Date/Time: 2025-03-06 - 13:58:53																				
<<<<<<<<< Report of MAP Node Point Requirements Pass/Fail and Corresponding Revised Values >>>>>>>>>>>>																				
Ingress Lane Id	Node Point #	Node Point Pos Req'd	Current Node Pos	Revised Node Pos	Node Pos Shift(m)	Lane Width Req'd	Current Width(cms)	Revised Width(cms)	Elevation Req'd	Current Elev(m)	Revised Elev(m)	Node Dist	Radius of Curve(m)	Distance	Required Length(m)					
1	0	-- Fail --	40.6924107	-111.544	40.6924147	-111.54356	0.5	-- Fail --	366	465	-- Pass --	2023	2004.3	-- Pass --	0	0				
1	1	-- Fail --	40.6924163	-111.54357	40.6924275	-111.54356	1.42	-- Fail --	366	336	-- Pass --	2023	2003.2	-- Fail --	53.7	36.3				
1	2	-- Pass --	40.6924539	-111.54347	40.6924501	-111.54348	0.88	-- Fail --	366	313	-- Fail --	2023	2002.9	-- Pass --	200.66	9.71				
1	3	-- Pass --	40.6925437	-111.54326	40.6925423	-111.54327	0.64	-- Fail --	366	329	-- Fail --	2023	2002.3	-- Pass --	154.88	20.12				
1	4	-- Pass --	40.6925702	-111.54318	40.6925705	-111.54318	0.53	-- Fail --	366	332	-- Fail --	2023	2002.1	-- Pass --	32.72	7.03				
1	5	-- Pass --	40.6925844	-111.54311	40.692583	-111.54311	1.02	-- Fail --	366	342	-- Fail --	2023	2001.9	-- Pass --	78.34	7.68				
1	6	-- Pass --	40.6925921	-111.543	40.6925919	-111.54301	0.78	-- Pass --	366	354	-- Fail --	2023	2001.6	-- Pass --	161.4	7.9				
1	7	-- Fail --	40.6925971	-111.54284	40.692599	-111.54284	0.58	-- Fail --	366	321	-- Fail --	2023	2001.1	-- Pass --	115.77	13.8				
1	8	-- Fail --	40.6926078	-111.54274	40.6926138	-111.54273	0.77	-- Fail --	366	335	-- Fail --	2023	2000.7	-- Pass --	30.35	8.68				
1	9	-- Pass --	40.6926337	-111.54266	40.6926375	-111.54265	0.96	-- Fail --	366	343	-- Fail --	2023	2000.4	-- Pass --	70.63	7.37				
1	10	-- Pass --	40.6926652	-111.54258	40.692663	-111.54259	0.44	-- Fail --	366	331	-- Fail --	2023	2000.2	-- Pass --	44.7	7.24				
1	11	-- Pass --	40.6927029	-111.54252	40.6927057	-111.54251	0.48	-- Fail --	366	301	-- Fail --	2023	1999.8	-- Pass --	43.62	6.8				
1	12	-- Pass --	40.6927399	-111.54247	40.6927437	-111.54247	0.53	-- Fail --	366	290	-- Fail --	2023	1999.6	-- Pass --	32.62	5.72				
1	13	-- Pass --	40.6927736	-111.54244	40.6927716	-111.54244	0.23	-- Fail --	366	292	-- Fail --	2023	1999.5	-- Pass --	0	4.56				
P/F - 10/4																				
P/F - 1/13																				
P/F - 2/12																				
P/F - 13/1																				
Tot: 142.91 200 @ 45 mph																				
2	0	-- Pass --	40.6923792	-111.544	40.6923778	-111.544	0.27	-- Fail --	366	336	-- Pass --	2023	2004.4	-- Pass --	0	0				
2	1	-- Pass --	40.6923828	-111.54373	40.6923845	-111.54372	0.97	-- Fail --	366	319	-- Pass --	2023	2003.7	-- Fail --	72.66	23.01				
2	2	-- Fail --	40.6924189	-111.54356	40.6924167	-111.54356	0.35	-- Fail --	366	314	-- Pass --	2023	2003.2	-- Pass --	0	14.69				
P/F - 2/1																				
P/F - 3/0																				
P/F - 2/1																				
Tot: 37.7 200 @ 45 mph																				
5	0	-- Pass --	40.6922421	-111.54413	40.692242	-111.54413	0.11	-- Pass --	366	365	-- Pass --	2023	2005.2	-- Pass --	0	0				
5	1	-- Fail --	40.6895164	-111.54412	40.6895131	-111.54412	0.46	-- Pass --	366	358	-- Pass --	2023	2016.7	-- Pass --	0	303.08				
P/F - 1/1																				
P/F - 2/0																				
P/F - 2/0																				
Tot: 303.08 200 @ 45 mph																				
6	0	-- Pass --	40.6922375	-111.54417	40.6922371	-111.54417	0.12	-- Pass --	366	367	-- Pass --	2023	2005.3	-- Pass --	0	0				
6	1	-- Fail --	40.6895164	-111.54416	40.6895125	-111.54416	0.56	-- Pass --	366	369	-- Pass --	2023	2016.8	-- Pass --	0	302.57				
P/F - 1/1																				
P/F - 2/0																				
P/F - 2/0																				
Tot: 302.57 200 @ 45 mph																				
4	0	-- Pass --	40.6922451	-111.54409	40.6922465	-111.54409	0.16	-- Fail --	366	290	-- Pass --	2023	2005.1	-- Pass --	0	0				
4	1	-- Fail --	40.6917506	-111.54409	40.6917452	-111.5441	0.7	-- Fail --	366	295	-- Pass --	2023	2007.1	-- Fail --	177.99	54.99				
4	2	-- Fail --	40.6916149	-111.54413	40.6916228	-111.54412	1.01	-- Pass --	366	350	-- Pass --	2023	2007.7	-- Pass --	0	15.39				
P/F - 1/2																				
P/F - 1/2																				
P/F - 3/0																				
P/F - 2/1																				
Tot: 70.38 200 @ 45 mph																				

Figure 17: Example - Truncated MAP Validation Report

2.  Click this button to start the web browser-based visualization of MAP validation assessment. As detailed in Section 2 concerning user input files, this procedure employs the JavaScript (.js) file created for the intersection in Module 3, along with a temporary JavaScript (.js) data array file produced during the MAP validation assessment process. The application process calls upon the default web browser to display the Google satellite view of the intersection, which is overlaid with lane boundary points, the calculated lane center, computed mid-points, and the lane node points as specified in the broadcast MAP. The text panel on left on the visualization provides complete detail about the broadcast MAP. Visualizer screen can be captured by pressing windows  key + Alt + PrtSc and can be saved in a desired folder. A sample visualization screenshot can be shown in Figure 18.

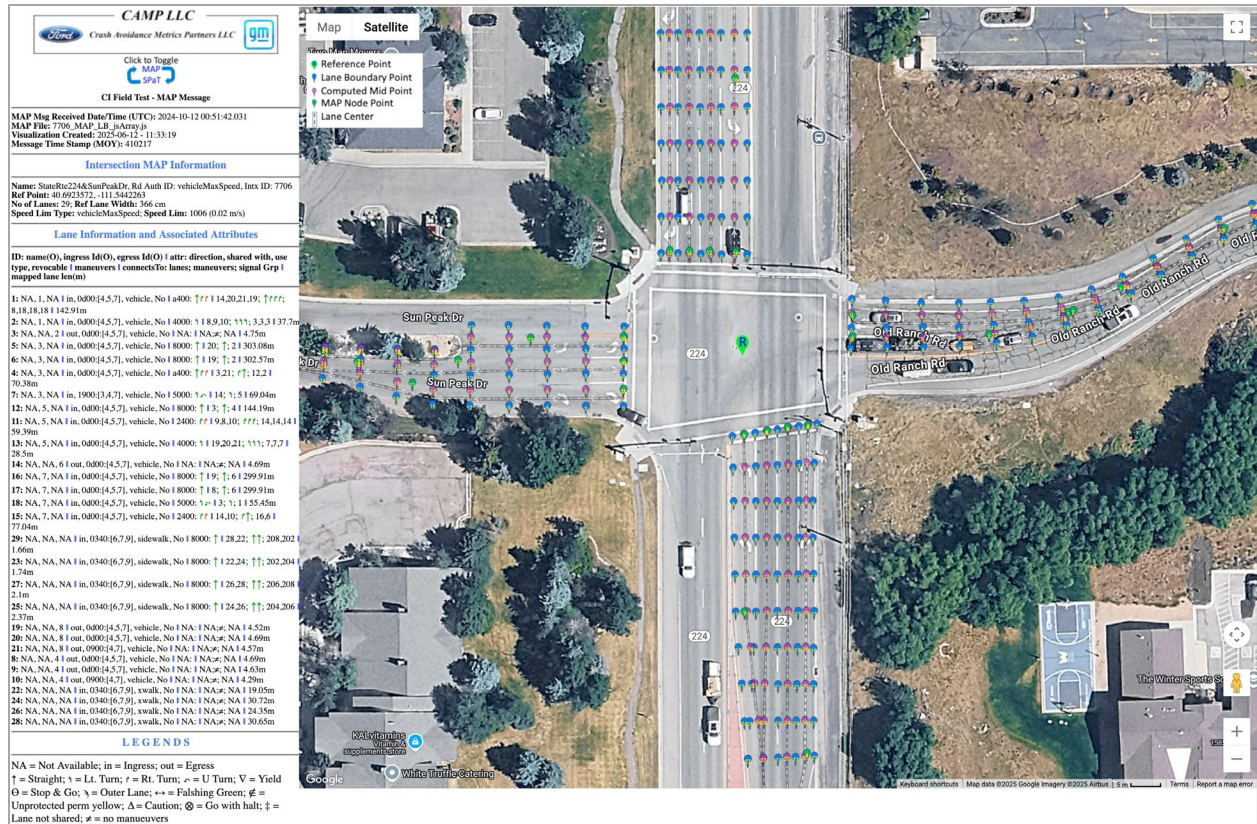



Figure 18: MAP Assessment Visualization Screenshot

3.  Click this button to exit the MAP validation assessment tool.

5 References:

1. J2735 - V2X Communications Message Set Dictionary
2. CTI 4501- Connected Intersections Implementation Guide. Publication pending.
3. CTI 4501/1 Connected Intersections Implementation Guide – SPaT Guidance. Publication pending.
4. CTI 4501/2 Connected Intersections Implementation Guide – MAP Guidance. Publication Pending.
5. CTI 4502 v01.00 Connected Transportation Interoperability (CTI) Connected Intersections Validation Report, February 2022, <https://www.ite.org/pub/?id=59A8D354-F7B1-6A18-6FCC-1CECE6ACDE5B>

Appendix A CI Performance Assessment Software Toolset

Table 2: Toolset Software Module Hierarchy

File Name	Description	File Type
<ul style="list-style-type: none"> CI_SPaT+MAP_Analysis_GUI_v1b.exe J2735_decoder-v2.0.5.exe 	<p>CI SPaT and MAP message analysis tool: (modules 0, 1, 2 and 3)</p> <p>Functions:</p> <ul style="list-style-type: none"> PCAP to JSON Conversion (module 0) <ul style="list-style-type: none"> Input: PCAP log file Output: Converted file in JSON Separate SPaT and MAP messages by intersection (Module 1) <ul style="list-style-type: none"> Input: Converted JSON file Output: Separated SPaT and MAP message files by intersection ID SPaT analysis (Module 2) <ul style="list-style-type: none"> Input: SPaT message JSON file for the intersection Output: <ul style="list-style-type: none"> Processed SPaT messages in CSV SPaT analysis summary report in CSV SPaT message periodicity plots in PNG SPaT data file in .js (JavaScript) MAP analysis (Module 3) <ul style="list-style-type: none"> Input: MAP message JSON file for the intersection Output: <ul style="list-style-type: none"> Processed MAP message in CSV MAP analysis summary report in CSV MAP data file in .js (JavaScript) MAP and SPaT message visualizer in a web browser 	<ul style="list-style-type: none"> Windows executables
<ul style="list-style-type: none"> RLVW_YP_Aanalysis_GUI_v2b.exe 	<p>SPaT yellow phase analysis tool (Module 4)</p> <p>Function:</p> <ul style="list-style-type: none"> Yellow phase analysis of controller data and SPaT messages for start and duration <ul style="list-style-type: none"> Input: <ul style="list-style-type: none"> Controller SPaT event data log file (CSV) SPaT messages in CSV (from module 2) 	<ul style="list-style-type: none"> Windows executable

File Name	Description	File Type
	<ul style="list-style-type: none"> – Output: <ul style="list-style-type: none"> ○ Yellow phase performance analysis in CSV ○ Yellow phase performance analysis summary in CSV ○ Yellow phase start time analysis plot ○ Yellow phase duration analysis plot 	
<ul style="list-style-type: none"> • CI_MAP_LB_Analysis_GUI_v3a.exe 	<p>CI MAP assessment tool (Module 5)</p> <p>Function:</p> <ul style="list-style-type: none"> • Intersection MAP geometry assessment using lane boundary data as ground truth <ul style="list-style-type: none"> – Input: <ul style="list-style-type: none"> ○ Lane boundary data file (CSV) ○ MAP data file in .js (JavaScript, from Module 3) – Output: MAP requirement pass/fail and suggested correction report (CSV) – Output: Visualization in a web browser <ul style="list-style-type: none"> ○ CI MAP overlay in Google satellite view ○ Lane boundary, computed mid-point and lane center overlaid MAP on Google satellite view 	<ul style="list-style-type: none"> • Windows executable
Folder Name	Supporting Folders and Files Description	File Type
<ul style="list-style-type: none"> • Summary_Report_Templates 	<ul style="list-style-type: none"> • File templates for generating SPaT and MAP performance analysis and summary reports 	CSV
<ul style="list-style-type: none"> • Visualizer 	<ul style="list-style-type: none"> • Software tools for generating web-based visualization 	Html, JavaScript
↳ Icons	<ul style="list-style-type: none"> • Various icons used for GUI and visualization 	png
↳ Temp_MAP_Viz	<ul style="list-style-type: none"> • Temporary folder to hold intermediate data array files from previous modules 	JavaScript

Traffic Signal Cabinet Logging Tool

Quick Reference Guide



prepared by **The Narwhal Group, LLC**
under the **Utah SMART Grant**

December 2024

Table of Contents

Introduction	1
How the tool works	1
Software architecture	4
Connect to the Traffic Signal Cabinet Logging Tool	5
Connect via IPv4	5
Connect via IPv6 local link	5
Access the UI	5
Access the tool via SSH	6
Change the IP address of the TSCLT	7
Deploying the tool in the field	7
Use case #1 - capture V2X and TSCBM messages	8
Use case #2 - capture V2X only	13
Using the Traffic Signal Cabinet Logging Tool	14
Cabinet tab	16
Cabinet configuration panel	17
Channels and Overlaps panel	17
Channels list	17
Overlaps list	18
Using overlaps for FYA	18
Data Collection tab	20
Data Collection Runs panel	20
Schedule list	23
Results list	23

Introduction

The *Traffic Signal Cabinet Logging Tool* (TSCLT) is a device used to collect data from a connected intersection (CI) which can then be analyzed by various CAMP applications to determine whether those messages meet the CTI 4501 specification.

This guide is meant for practitioners who will be deploying the tool in (or near) a traffic signal cabinet for a connected intersection, that is, an infrastructure system that broadcasts signal, phase and timing (SPaT), mapping information and position correction data to vehicles. The tool's software is hosted on a device capable of receiving over-the-air V2X messages from connected intersections, typically an OBU.

How the tool works

Once the tool is configured for a given CI cabinet, messages are recorded according to a given schedule and can then be downloaded once the data collection has been completed. The TSCLT is capable of collecting the following data at a given connected intersection:

- Serial data from a BIU/SIU bus using a SDLC adapter and special cable connected directly to the cabinet's serial bus which is both logged as raw data and converted into an ATSPM-like format with the help of cabinet-specific configuration file;
- Over-the-air (OTA) V2X messages (MAP/SPaT/BSM,TIM,RTCM/SRM/SSM, etc.) broadcast by equipped vehicles and connected intersections in range, received by the wireless V2X network interfaces, and logged in pcap (<https://en.wikipedia.org/wiki/Pcap>) format;
- Traffic signal controller Battelle Messages (TSCBM) sent from the traffic signal controller and logged in pcap format;
- Immediate forward messages (IFM) sent from the traffic signal controller or ECLA logged in pcap format.

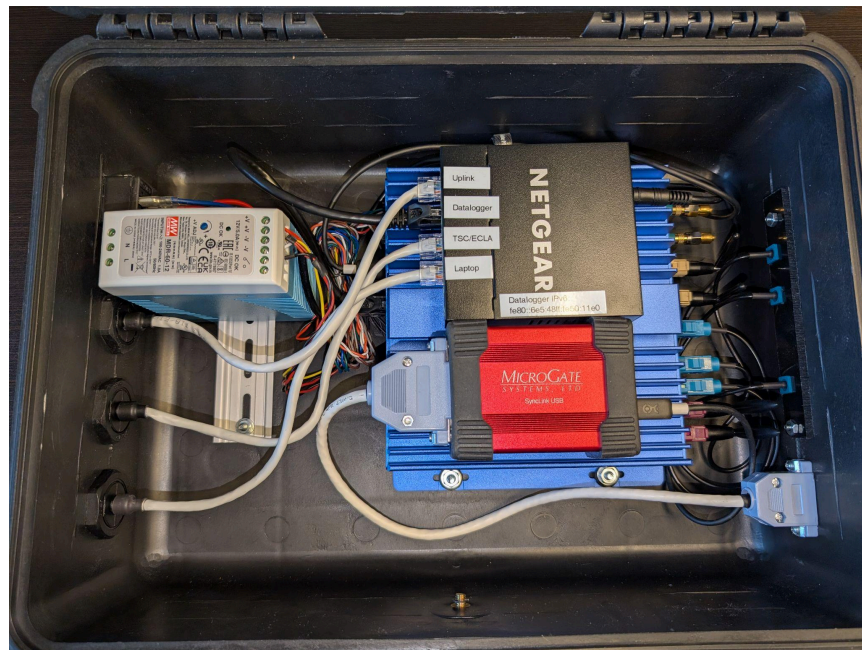
Strictly speaking, the CAMP analysis tools currently only use the first two outputs, the ATSPM-like data and the over-the-air data. However, capturing the other two data streams, if possible, might help in debugging any issues that may arise in the analysis of the generated SPaT messages of the connected intersection under test.

The TSCLT is housed inside a polypropylene suitcase that can be placed into a traffic signal cabinet and also supports connecting the V2X equipment antenna and other equipment required to do data captures for the connected intersection. The case contains the following components:

- Cohda OBU
- MicroGate SyncLink USB (<https://microgate.com/#/USBAdapter/>)
- 5 port Gigabit managed switch

- Power supply
- All of the cables and accessories required to connect the TSCLT to the traffic signal cabinet
 - AC power cord
 - SDLC cable
 - SDLC Y cable
 - V2X antenna
 - CAT 6 ethernet cables (qty. 2)
 - Roll of double sided tape (to temporarily affix the V2X antenna to non-magnetic cabinets)

There are connectors on the outside of the case that enable connection to the components inside the case. The connections include AC power, V2X antenna (V2X and GPS), the SDLC cable between the cabinet and the SyncLink, and RJ-45 ports for connecting to the cabinet's network switch, TSC/ECLA and a laptop to run the TSCLT UI.



Interior of TSCLT Suitcase



Left Side of TSCLT Suitcase



Right side of TSCLT suitcase



Software architecture

The software runs on the Cohda OBU and consists of a web-based user interface and a backend service.

[architecture diagram]

The user interface is where a user can configure cabinet configurations, schedule and monitor data collections, and manage the collected data, i.e., download, delete, etc.

The backend service performs the data collections, manages the data, accepts and implements commands received from the user interface.

The system is designed so that a user does not have to be logged into the system in order to perform data collections. Data collections are scheduled to have a starting and ending time, making it convenient to collect data during or prior to an event such as a timing plan change or some other transitional period. The system also supports starting a data collection *now*, and ending at a specific time. Any running collection can also be interrupted which simply stops the data collection process at a given point but preserves all collected data.

When a data collection is started, an application is launched that starts one or more applications to start collecting data. This application monitors these subprocesses waiting for them to exit at which time the application also exits and the data collection is considered complete. The system is designed such that only one data collection can be performed at a time.

Connect to the Traffic Signal Cabinet Logging Tool

The TSCLT must be configured before data collection can take place. In order to configure the tool a laptop or other computer must be connected to it to access the UI and optionally to set the IP address of the tool. There are two methods to connect to the tool via ethernet.

Connect via IPv4

- Plug an ethernet patch cable into the TSCLT's Laptop port and plug the other end into your computer.
- The default IPv4 address of the TSCLT is 192.168.0.254 /24.
- Set your computer's IP address to be on the same subnet as the TSCLT. (example: set your laptop to 192.168.0.100, netmask 255.255.255.0).

Connect via IPv6 local link

Connecting via IPv6 works only when your computer is directly connected to the tool or when your computer is connected to the same network switch as the TSCLT tool (local connection). The advantage is that the IPV6 local link address of the tool is always the same regardless of the IPv4 address.

- Plug an ethernet patch cable into the TSCLT's Laptop port and plug the other end into your computer.
- The IPv6 local link address is unique to each device. Inside the TSCLT suitcase there is a sticker with the IPV6 local link address printed on it.
(example IPv6 address: fe80::6e5:48ff:fe50:11e0)

Access the UI

Access the TSCLT UI by typing the tool's IPv4 address (192.168.0.254) into a web browser's address bar. See the *Using the Traffic Signal Cabinet Logging Tool* section of this guide for more information on using the UI.

The UI can also be accessed via the IPv6 local link address on Windows computers. The format for the address to be typed into the browser is: `http://[IPv6-local-link-address]` (note: square brackets are required).

Example: `http://[fe80::6e5:48ff:fe50:11e0]`

The UI credentials are:

Username: smart

Password: Sp@tL0gger

Access the tool via SSH

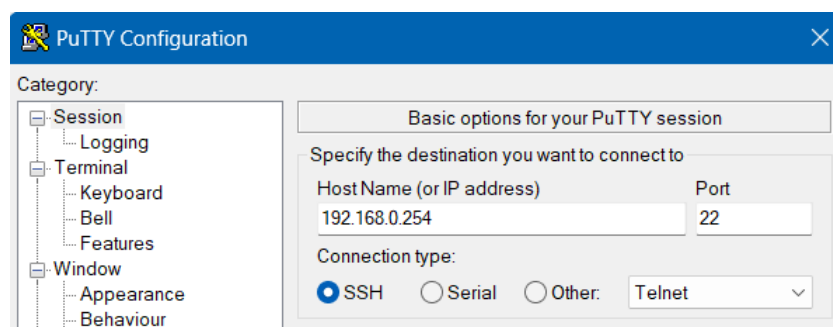
Connect to the tool via SSH to set the IPv4 address of the tool and to verify that TSCBM messages are being received (see the *Deploying the tool in the field* section of this guide). On Windows computers an SSH client such as PuTTY can be used to connect to the tool for this purpose.

When connecting via IPv4, use the IPv4 address and port 22. When connecting via IPv6 local link, a percent symbol (%) and the device ID (or Zone Index) of your computer's ethernet port must be appended to the local link address.

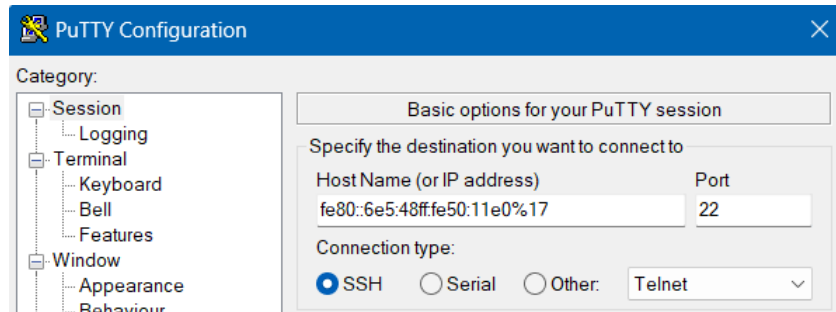
On Linux computers `eth0` is a common device ID for the main ethernet port. On Windows computers, the ethernet device ID will be numeric. Use the ***ipconfig*** command in a Windows command prompt to find your computer's ethernet port device ID. In the example below the device ID of Ethernet 5 is 17:

```
C:\Users\rkoeber>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet 5:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::db4b:5f53:7d72:8ceb%17
    IPv4 Address. . . . . : 192.168.200.129
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.200.1
```



SSH via IPv4 using PuTTY



SSH via IPv6 using PuTTY

SSH credentials are:

Username: user

Password: user

Change the IP address of the TSCLT

It may be necessary to change the IPv4 address of the TSCLT so it can connect to an existing network. Set the new IP address by connecting to the tool via SSH and running the following commands to set the IP address, netmask and gateway. In the example they are set to 192.168.0.254, 255.255.255.0, 192.168.0.1, respectively.

```
login as: user
user@192.168.199.201's password:
Welcome to Cohda Wireless MK6 (MK6)

* Documentation:  https://support.cohdawireless.com
Last login: Thu Jan 16 00:04:02 2025 from 192.168.200.129
root@MK6:~# fw_setenv static_ip_addr "192.168.0.254"
root@MK6:~# fw_setenv static_ip_mask "255.255.255.0"
root@MK6:~# fw_setenv static_ip_gw "192.168.0.1"
root@MK6:~# reboot
```

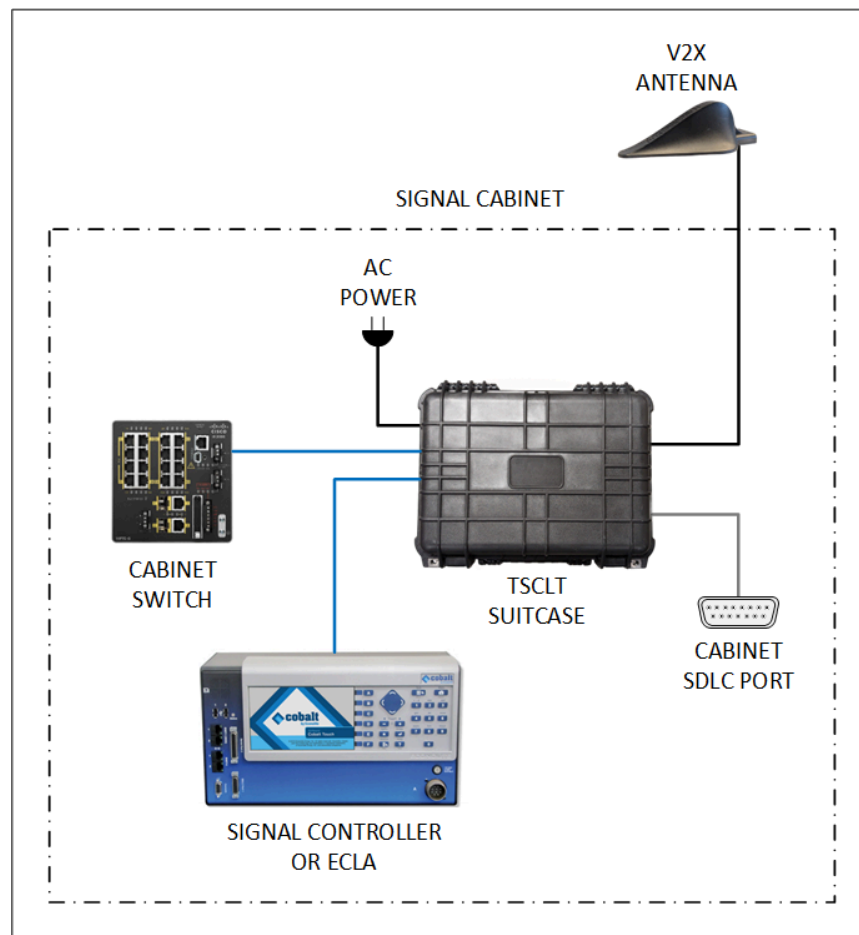
The tool will reboot and the IPv4 address, netmask and gateway will be changed to the new values.

Deploying the tool in the field

The following are examples of how to deploy the TSCLT in order to collect specific sets of data.

Use case #1 - capture V2X and TSCBM messages

In this use case the TSCLT will be connected to the cabinet's internal network so that it will be possible to capture V2X OTA messages, BIU/SIU messages from the SDLC bus as well as TSCBM messages sent from the traffic signal controller to the RSU/ECLA. For this scenario, the TSCLT will be connected to both the cabinet's internal IP network using a managed switch and the traffic signal controller's SDLC bus.

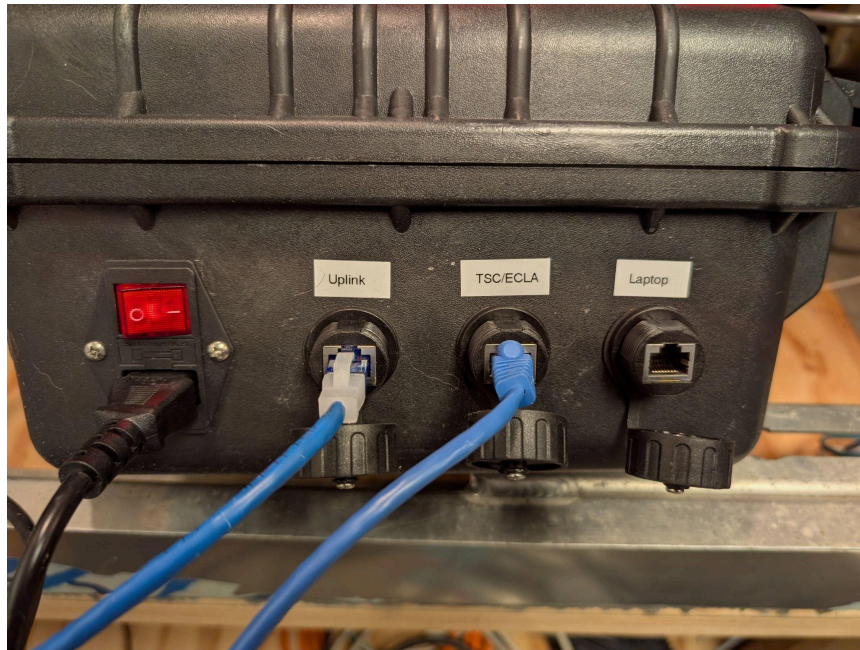


Connection Diagram for Capturing V2X and TSCBM

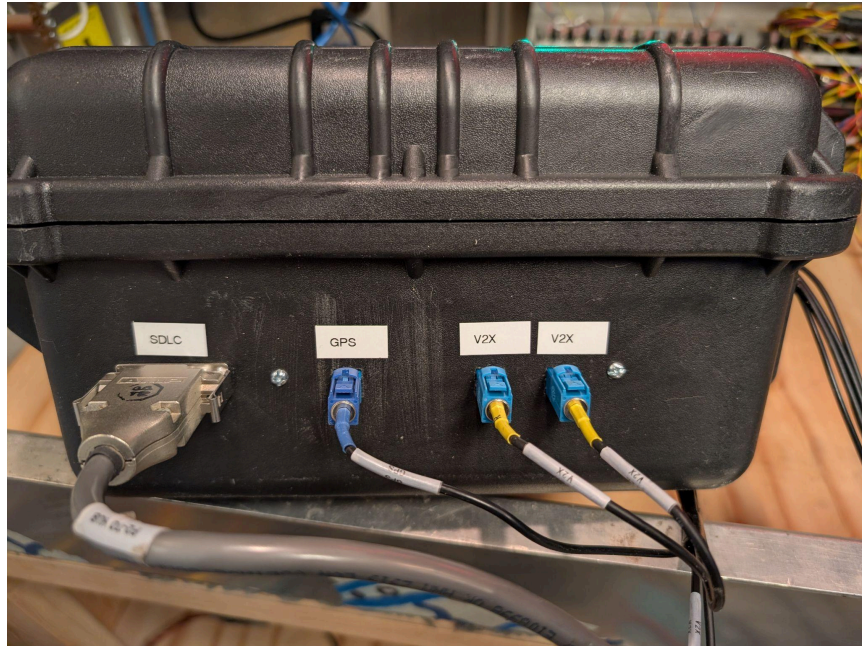
The managed switch is used to make it possible to capture the TSCBM messages being sent from the traffic signal controller to the RSU or ECLA. Perform the following steps to connect the TSCLT to the cabinet:

1. Connect the TSCLT power cord to a 120V AC outlet.
2. Attach the V2X antenna to the top exterior of the signal cabinet.
 - a. Plug the V2X cables (aqua blue) into the V2X ports on the TSCLT (any two V2X cables).
 - b. Plug the GPS cable (dark blue) into the GPS port on the TSCLT.

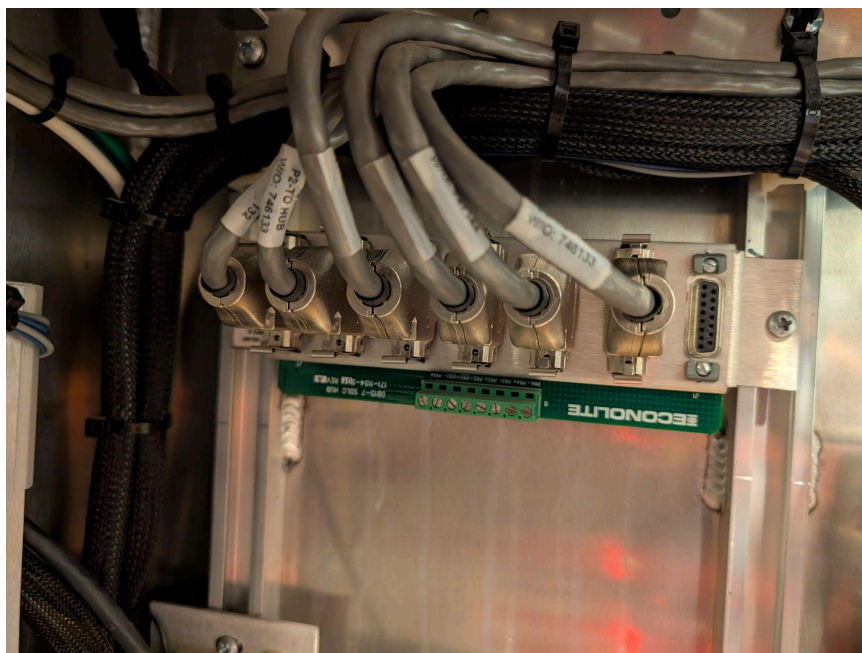
3. Plug the SCLC cable into the SDLC port on the TSCLT and into the cabinet's SDLC bus.
Note: An SDLC "Y" cable may be required to connect to the cabinet SDLC bus if there is not an unused SDLC port in the cabinet.
4. Disconnect the traffic signal controller or ECLA ethernet cable from the signal cabinet's network switch, noting the port on the cabinet's switch. Plug an ethernet cable into that same port on the cabinet switch and plug the other end into the UPLINK port on the TSCLT suitcase.
5. Plug the ethernet cable from the traffic signal controller or ECLA into the TSC/ECLA port on the TSCLT suitcase.
6. Turn on the power switch on the left side of the TSCLT.



TSCLT left side connections



TSCLT right side connections



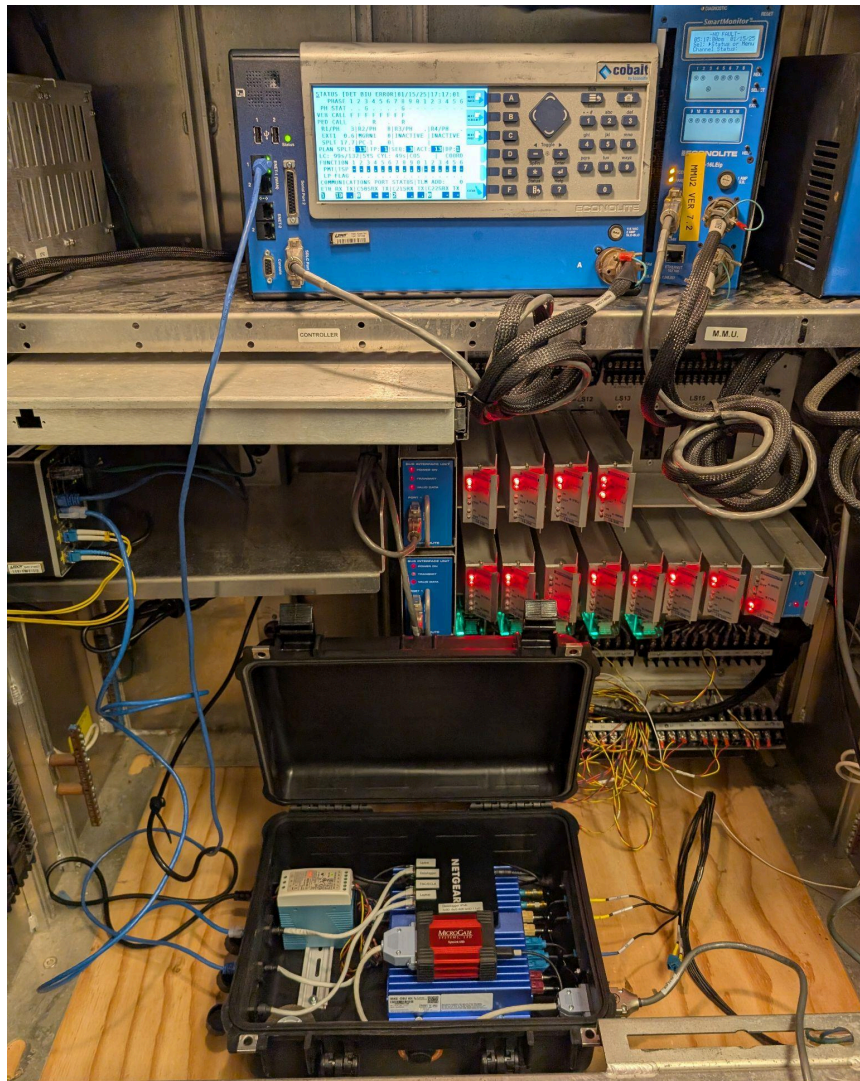
Cabinet SDLC bus with empty port



SDLC cable to TSCLT (right most cable)



V2X antenna placement (lab environment shown)



TSCLT connected to signal cabinet (lab environment shown)

To test that the managed switch is mirroring traffic from the traffic signal controller, log into the TSCLT and run the following command:

```
root@MK6:~# tcpdump -i eth0 port 6053
tcpdump: verbose output suppressed, use -v or -vv for full protocol
decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
21:22:07.494270 IP 10.213.5.63.40810 > 10.213.5.62.6053: UDP, length 245
21:22:07.593970 IP 10.213.5.63.40810 > 10.213.5.62.6053: UDP, length 245
21:22:07.694330 IP 10.213.5.63.40810 > 10.213.5.62.6053: UDP, length 245
21:22:07.794240 IP 10.213.5.63.40810 > 10.213.5.62.6053: UDP, length 245
21:22:07.893884 IP 10.213.5.63.40810 > 10.213.5.62.6053: UDP, length 245
```



```

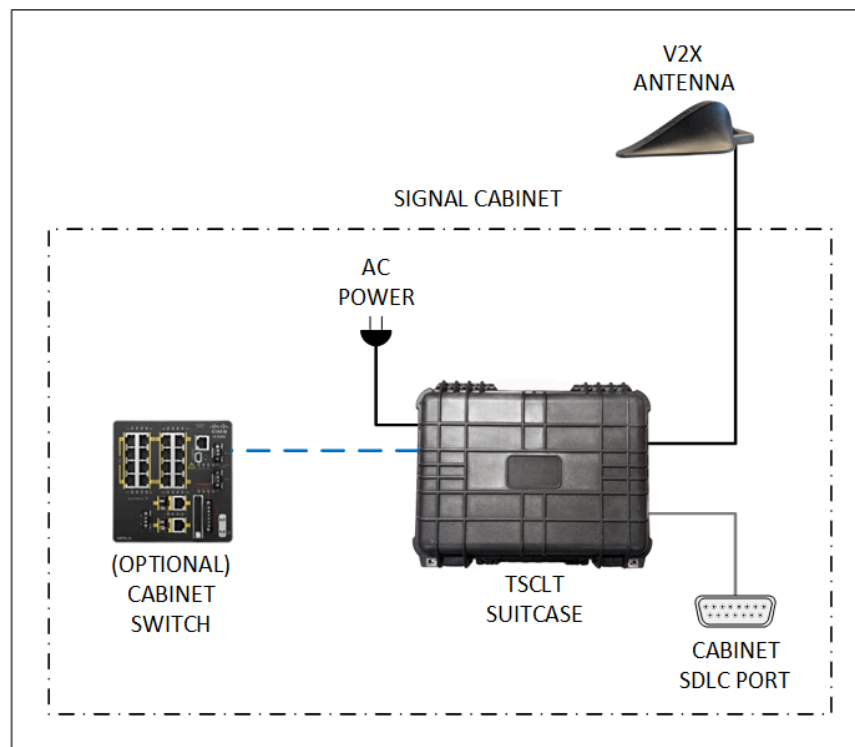
21:22:07.994212 IP 10.213.5.63.40810 > 10.213.5.62.6053: UDP, length 245
:
^C
57 packets captured
226 packets received by filter
169 packets dropped by kernel
root@MK6:~#

```

This command assumes the traffic signal controller is sending TSCBM to port 6053 on a given IP address. Adjust the port number if it is being sent to a different port.

Use case #2 - capture V2X only

In this use case, the TSCLT will be used to only capture V2X OTA messages and BIU/SIU messages from the SDLC bus. For this scenario, the connection to the Signal Controller or ECLA is omitted and only the connection from the TSCLT to the SDLC bus is required. Optionally the Uplink port on the TSCLT may be connected to the cabinet network switch for remote access to the suitcase.



V2X Only Capture Diagram

Perform the following steps to connect the TSCLT to the cabinet:

1. Connect the TSCLT power cord to a 120V AC outlet.

2. Attach the V2X antenna to the top exterior of the signal cabinet.
 - a. Plug the V2X cables (aqua blue) into the V2X ports on the TSCLT (any two V2X cables).
 - b. Plug the GPS cable (dark blue) into the GPS port on the TSCLT.
3. Plug the SCLC cable into the SDLC port on the TSCLT and into the cabinet's SDLC bus.
Note: An SDLC "Y" cable may be required to connect to the cabinet SDLC bus if there is not an unused SDLC port in the cabinet.
4. (Optional) Plug an ethernet cable into the Uplink port on the TSCLT and into an unused port on the cabinet network switch. This will allow remote access to the tool.
5. Turn on the power switch on the left side of the TSCLT.

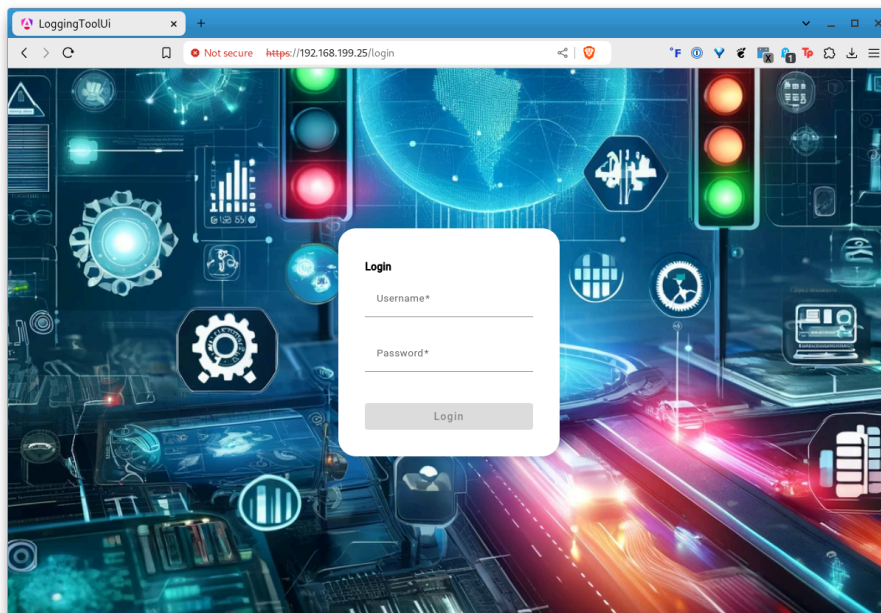
Using the Traffic Signal Cabinet Logging Tool

To use the tool, a knowledge of how a given traffic signal cabinet's load switches are configured and used by the traffic signal is required. This is known as the *channel and overlaps configuration*.

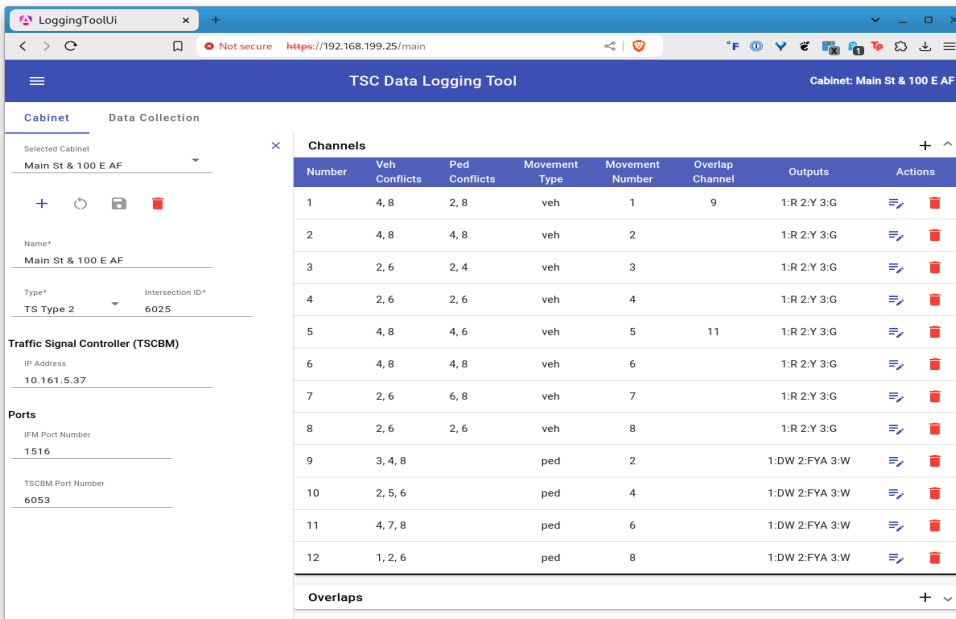
Channel definitions in the TSCLT are essentially a one for one representation of a given load switch installed in the cabinet and commanded by the traffic signal controller. Channel numbers correspond to a given position of a load switch in a given load bay according to the [cabinet standard]. For example, for an NEMA Type 2 cabinet, channel 5 corresponds to the fifth load switch in bay 1, and channel 10 corresponds to the second load switch in bay 2.

In a typical 4 approach, 8 phase intersection with pedestrian crossings, you'll have 12 defined channels. Overlap definitions can also be defined but their only use in this application is modeling flashing yellow arrows.

At startup, the logging tool user interface shows a login dialog:



Log in using the credentials provided and the full user interface will be shown:



The user interface consists of two tab groups, *Cabinet* and *Data Collection*. The *Cabinet* tab is where cabinets are managed, i.e. displayed, added, updated, and deleted. The *Data Collection* tab is where data collections are managed, scheduled, run, and collection results downloaded.

Cabinet tab

Within the TSCLT, a *cabinet* contains the definition of all of its load switches, their functions as well as any other site-specific definitions such as its name, IP address of the traffic signal controller, etc. The Cabinet tab allows users with sufficient privilege to add cabinets, modify or delete their definitions and update site-specific information for a cabinet.

The main parts of the Cabinet tab are described below.

Cabinet configuration panel

1. Current cabinet drop down - allows a user to select a cabinet from the list of configured cabinets. Selecting a cabinet from the list makes it the current cabinet being shown in the user interface, including on the *Data Collection* tab.
2. Add cabinet - Shows the Add Cabinet dialog allowing a new cabinet to be created.
3. Revert - if there are unsaved edits to a cabinet configuration, excluding channel changes, they can be reverted to the previously saved state.
4. Save - save edits to a cabinet configuration.
5. Delete - delete a cabinet from the TSCLT.
6. Name - name of cabinet.

7. Type - cabinet type.
8. Intersection ID - an integer that represents an intersection's identifier.
9. Traffic Signal Controller - IP address of device that is transmitting TSCBM, typically the traffic signal controller.
10. IFM port number - UDP IP port number where immediate forward messages are sent to be broadcast.
11. TSCBM port number - UDP IP Port number that is transmitting Traffic Signal Controller Battelle Messages.

Channels and Overlaps panel

The panel shows the configured channel and overlaps for the selected cabinet.

Channels list

The following columns are shown in the *Channels* list, those marked with an asterisk are required:

1. Number* - channel number for association with a given load switch
2. Veh Conflicts - any vehicle conflicts associated with the associated movement type and movement number;
3. Ped Conflicts - any pedestrian conflicts associated with the associated movement type and movement number;
4. Movement Type* - type of traffic movement associated with a given channel;
5. Movement Number* - traffic movement (phase) associated with a given channel, along with movement type, , this is the phase number used in the ATSPM data file output;
6. Overlap Channel - which overlap channel, if any, is used in conjunction with this channel;
7. Outputs* - what each output on the load switch represents, i.e., red, yellow, green, walk, don't walk, flashing yellow arrow, flashing don't.

The *Actions* column contains buttons which allow a user to edit or delete a given channel. Above the *Channels* list is an add button that allows users to add channels to a cabinet's configuration.

Overlaps list

The following columns are shown in the *Overlaps* list, all of which are required:

1. Name* - name of overlap
2. Channel* - channel number for association with a given load switch
3. Opposing Movement* - movement (phase) which this overlap is active;
4. Types - the purpose of this overlap in the context of the data collection we are performing, we support only pedestrian and flashing yellow arrows.

The *Actions* column contains buttons which allow a user to edit or delete a given overlap. Above the *Overlaps* list is an add button that allows users to add overlaps to a cabinet's configuration.

Using overlaps for FYA

Sometimes flashing yellow arrows (FYA) for a permissive left turn use an overlap to make them flash, typically during an opposing pedestrian phase. In this case, the channel and the overlap should be associated in order for the data to be recorded properly. For example, suppose that channel 1 is a left turn and it uses a FYA during pedestrian phase 2. Assuming a 4 approach, 8 phase intersection with standard overlap configuration, channel 1, i.e., vehicle movement 1, should add an overlap channel for ped phase 2, i.e., channel 9:

The screenshot shows the 'Edit Channel' dialog box with a close button (X) in the top right corner. The 'Number*' field contains the value '1'. The 'Overlap Channel' dropdown menu is open, showing a list of options: '9' (which is highlighted with a blue checkmark), '10', '11', and '12'. The 'Vehicle Conflicts' field contains the value '4, 8'. The 'Movement' section has a 'Movement Type*' dropdown menu set to 'veh'.

In addition, channel 9 should add the output type FYA where that is wired on the load switch, in most case pin 2:

The screenshot shows the 'Edit Channel' dialog box with a close button (X) in the top right corner. The 'Number*' field contains the value '9'. The 'Overlap Channel' dropdown menu is open, showing a list of options: '9' (which is highlighted with a blue checkmark), '10', '11', and '12'. The 'Vehicle Conflicts' field contains the value '3, 4, 8'. The 'Ped Conflicts' field is empty. The 'Movement' section has a 'Movement Type*' dropdown menu set to 'ped' and a 'Movement Number*' field containing the value '2'. The 'Movement Outputs' section has a plus sign (+) in the top right corner. It contains two rows of output configurations: the first row has 'Number*' set to '1' and 'Output Type*' set to 'DW'; the second row has 'Number*' set to '2' and 'Output Type*' set to 'FYA'. Each row has a close button (X) in the top right corner.

And lastly, the overlap for channel 9 should include fya in the *overlap types* it supports:

Edit Channel Overlap [X]

Name*
A

Channel Number*
9

Channel Opposing Movement*
2

Overlay types*
ped, fya

- ☒ ped
- ☒ fya

Data Collection tab

Data collection is performed for a given cabinet by first defining what needs to be collected, scheduling or simply starting a collection, and then downloading the files created as part of the data collection. The three panels shown on this page reflect each of those steps in the process.

Data Collection Runs panel

The panel shows a list of data collection configurations for the selected cabinet. The following columns are shown in the list:

1. Name - the name of the collection configuration;
2. Result location - the root directory on the host (OBU) where files are stored; this directory name plus the intersection identifier will be the folder where the collections for this cabinet are stored;
3. ATSPM - if checked, collection serial bus data in ATSPM-like format;
4. TSCBM - if checked, collect TSCBM data in pcap format;
5. IFM - if checked, collect IFM data in pcap format;
6. OTA - if checked, collect V2X messages received over-the-air in pcap format

The *Actions* column contains buttons which allow a user either start, edit or delete a data collection. If the Start button is selected, a dialog is shown to allow the user to select when the collection will end:

Start Collection Run Now

×

Collection Name*

CAMP only

Start: Now

Select a time for the collection run to stop:

Stop*

01/09/2025

Time*

07:15 PM

Reset

Start

Cancel

Above the list is an add button that allows users to add data collections for the selected cabinet:

Add New Collection Run

×

Name*

CAMP only

Final File Destination

/mnt/rw/tscit

Collect the following data:

☒ ATSPM

☐ TSCBM

☐ IFM

☒ OTA

Schedule a start time (Optional):

Start Date

Time

End Date

Time










Save

Cancel

If the schedule section is filled in it will also schedule the data collection to start at a given time and end at a given time.

Schedule list







The Schedule shows data collections that are running now and are scheduled to be run in the future. When a data collection starts, an entry is shown in the Schedule and Results lists related to the data collection:

Data Collection Runs							+ ^
Name	Result Location	ATSPM	TSCBM	IFM	OTA	Actions	
CAMP full	/mnt/rw/narwhal/tscit	✓	✓	✓	✓	  	
Schedule							+ ^
Name	Owner	Result Location	Start	Stop	Status	Actions	
CAMP full	admin	/mnt/rw/narwhal/tscit	01/09/2025 06:16 PM	01/09/2025 06:20 PM	Running	  	
Results							^
Name	Owner	Start	Stop	Status	Actions		
CAMP full	admin	01/09/2025 06:16 PM	01/09/2025 06:20 PM	Running	  		

While the collection has status *Running* in the *Schedule* list, it can be stopped by selecting the Stop button.

Results list

The Results list shows information regarding previous data collection operations and the data collection run that is currently active, if one exists. When a data collection run has been completed, it will be removed from the Schedule list and the buttons in the Results list related to the completed collection will become active:

Data Collection Runs							+ ^
Name	Result Location	ATSPM	TSCBM	IFM	OTA	Actions	
CAMP full	/mnt/rw/narwhal/tscit	✓	✓	✓	✓	  	
Schedule							+ ^
Name	Owner	Result Location	Start	Stop	Status	Actions	
Results							^
Name	Owner	Start	Stop	Status	Actions		
CAMP full	admin	01/09/2025 06:16 PM	01/09/2025 06:20 PM	Complete	  		

At this point, the collected data has been written to the specified host directory and can be downloaded, a summary viewed, or it can be deleted from the host.

To download the data, select the download button and select which files you wish to download:

Select files to download

- ☒ 7704-atspm.csv 48.53 KB 1/6/2025
- ☒ 7704-ifm.pcap 42.41 MB 1/6/2025
- ☒ 7704-logger.log 18.57 MB 1/6/2025
- ☐ 7704-rmnet_data15-ota.pcap 26.54 KB 1/6/2025
- ☒ 7704-rmnet_data16-ota.pcap 31.75 MB 1/6/2025
- ☒ 7704-tscbm.pcap 18.20 MB 1/6/2025
- ☒ 7704.json 2.47 KB 1/6/2025

Download

Cancel

SCMS Manager Intersection Validation and Certificate Issuance Policy

SCMS Manager

September 19, 2024

1 Overview

Successful connected intersection deployment and operation depends on trust among production vehicles and a wide variety of transportation infrastructure. The SCMS architecture supports trust by providing a collection of trusted root certificates operated by authorized vendors who agree to implement a common set of policies. However, security infrastructure alone can only provide assurance for the integrity of broadcast messages as they travel from a sender to a collection of receivers. Assurance that the data content of those messages is consistently accurate and aligned with physical signals and signage requires validation.

This document describes the role of the SCMS Manager in the implementation and enforcement of validated intersections. SCMS Providers which are authorized by the SCMS Manager to issue certificates to V2X stations must support the intersection validation procedures defined in this policy if they intend to issue credentials for validated intersections.

1.1 Connected Signalized Intersection Validation

A signalized intersection consists of a collection of equipment and traffic control signals that safely coordinates the flow of traffic through a shared segment of roadway. A connected signalized intersection (CSI) is defined as an infrastructure system that broadcasts signal, phase, and timing (SPaT), mapping information and position correction data. Intersection validation is a set of procedures that test the conformance of the broadcast data to a set of performance parameters. A CSI that has passed the required validation tests is classified as *validated*. Any CSI that has not been tested or that has failed a validation test is classified as *unvalidated*.

The digital messages that are broadcast by a connected intersection are typically constructed, signed, and broadcast by a Roadside Unit (RSU). In order to be trusted by other V2X devices, an RSU must be issued certificates by an authorized SCMS Provider. The certificates issued to an RSU can have specific permissions enabled by the SCMS Provider.

1.2 Concept of Operation

As a certificate authority (CA), an SCMS Provider is responsible for evaluating the capabilities and security status of a V2X system and issuing appropriate certificates for individual devices. In the case of a validated intersection, the requirements for evaluating the system is extended to include the review and monitoring of reports containing results of measurements collected to evaluate the level of consistency (or validity) of broadcast data when compared to the “ground truth” in the physical environment. In performing this function, the only actions that the SCMS provider can take is to issue certificates with appropriate properties, monitor operations and decide if it is necessary to block short-term certificate updates to a device or revoke a system’s permissions completely.

A high-level view of the process for validated intersection is as follows:

1. An IOO¹ submits an enrollment request to an SCMS Provider for an RSU, indicating that the intersection will be operated in *validated* mode.
2. The SCMS Provider will apply this policy to evaluate the merits and capabilities of the intersection and the RSU. If the functional conditions for validation are met, then the SCMS Provider will issue an enrollment certificate with the required SSPs needed to enable the broadcast of validated messages.
3. The IOO will begin operation of the RSU by broadcasting messages that have the **validation_enabled** indicator absent, meaning that the content may not be treated as validated.
4. The IOO will use a certified tool (or engage a certified testing resource) to collect data on the performance of the intersection. The data collection process will provide detailed reports which may be used by the IOO (or service provider) to adjust or correct any operational issues.
5. Once the IOO is satisfied that the intersection is operating correctly, a machine-readable Validation Report will be produced and delivered to the SCMS Provider that issued the RSU certificates.²
6. The SCMS Provider will receive the report and confirm that the summary metrics were derived using a certified tool and that the results meet the requirements for validation. If the report is accepted, then the SCMS Provider responds back to the IOO that the intersection may activate the **validation_enabled** content in broadcast messages.
7. The IOO will activate a continuous monitoring service which will collect data from the intersection. The monitoring service will send periodic reports to the SCMS Provider, confirming that it is active and that the intersection is operating normally.

2 Message Components and Intersection State

A connected intersection may broadcast a variety of message types. In order to support specific safety applications, such as Red Light Violation Warning (RLVW), a CSI must broadcast SPaT, MAP, and RTCM as defined in SAE J2735, “V2X Communications Message Set Dictionary”.

Each of the required messages may be broadcast in a *validated* or *unvalidated* state. All three of the required messages (SPaT, MPA, and RTCM) must be present and all three must be operating in *validated* mode in order for the entire intersection to be declared to be *validated*.

An intersection may operate in a mode where one or more of the required message types do not have validation enabled. In this case the intersection is declared to be in *unvalidated* mode. To make that more clear, consider that the \wedge symbol represents a logical AND operation. Then the state of validation for an intersection can be assigned as:

$$[intersection_state] = [SPaT_state] \wedge [MAP_state] \wedge [RTCM_state]$$

A CSI can reliably support critical safety applications, such as RLVW, when all three required message types (SPaT, MAP, and RTCM) are present and all three are operating in *validated* mode.

3 Message Permissions and Operating State

Each of the required message types (SPaT, MAP, and RTCM) has a defined structure for Service-Specific Permissions (SSP) values which includes a **validation_supported** field. It is the responsibility of the SCMS Provider to apply this policy when issuing certificates that include the **validation_supported** SSP indicators for SPaT, MAP, and RTCM.

4 Message Permissions and Message Body Content

In addition to the **validation_supported** indicator in the SSP, each of the required messages has a **validated_mode** field as part of the message body. This field is used to indicate the current operating mode

¹Or a service provider operating on behalf of an IOO.

²This is a consolidated report that contains results for SPaT, MAP, and RTCM.

of the RSU at the time when the message was broadcast.

When this flag is present in the message body, then the `validation_supported` SSP flag must also be enabled. A certified and compliant RSU shall never sign a message that has the `validated_mode` flag present if the currently active application certificate does not have the `validation_supported` flag set.

SSP Content	Message Body	Meaning
<code>validation_supported</code> present	<code>validated_mode</code> present	message content validated
<code>validation_supported</code> present	<code>validated_mode</code> absent	message content not validated
<code>validation_supported</code> absent	<code>validated_mode</code> absent	message content not validated
<code>validation_supported</code> absent	<code>validated_mode</code> present	misbehavior

5 Three types of reports are sent to an SCMS Provider

- Initial validation report (one-time or as-needed)
 - Validate SPaT accuracy + latency, MAP data accuracy, and RTCM performance
- Continuous monitoring update (weekly)
 - Capture BSMs from vehicles as they drive through the intersection
 - Analysis shows how human drivers respond to traffic signal changes
- On-site inspection (annual or as-needed)
 - Confirm that the system is working, update any data on the roadway or signal controller

6 Intersection Validation Requirements

- Initial validation measurements to be collected using a Certified test tool or Certified lab
 - Certification to be issued by independent review (OmniAir or other)
 - DOT can use a certified tool to collect data on their own intersections (self-validation)
 - DOT can contract with a certified lab to have this done (third-party validation)
 - Reports to be submitted directly from the certified tool or lab to an SCMS Provider that has a contract with the DOT (reports can be sent to multiple SCMS providers)
 - A validated intersection must use a certified RSU
- Initial validation metrics must include all operational modes
- All validated intersections must be independently tested (for a period of time)
 - Over time, we may allow for “type validation” that applies to similarly configured systems or a sampling plan
- Not all connected intersections will be validated
 - DOTs can operate non-validated intersections for internal / local use *Production vehicles may use non-validated data as informative only, or ignore
- Continuous Monitoring with a Certified utility is required to maintain validation
 - Continuous monitoring equipment must be type Certified by a lab
 - CIMMS is one type of monitoring that may be approved, other methods may be added over time
- Continuous Monitoring can trigger an immediate change of state
 - When the monitoring system detects a condition that is out of specification, it can automatically trigger the RSU to switch to standby mode (no broadcast)
 - Response time to switch to standby to be < 10 s (need to define how to measure this)
 - The switch to standby will also notify DOT that the switch has occurred
 - An on-site inspection is needed to recover from standby mode
 - After a switch to standby, intersection may transition to a validated or invalidated state
- Continuous Monitoring to send periodic reports to an SCMS provider

- Reports to be submitted weekly (aligned with the certificate top-off cycle)
 - Reports show that the monitoring system is on and working
 - Report submission and acceptance to be automated
 - Absence of a scheduled report will trigger SCMS provider to notify DOT
 - Failure to correct report delivery to cause SCMS provider to block the impacted RSU
- On-Site inspection to be performed annually
 - Each validated intersection must be physically inspected at least once per-year
- On-Site inspection requires a subset of the initial validation test
 - The on-site inspection requires a minimally-invasive set of measurements of the intersection
 - Shall include receiving and validating RSU broadcasts
 - Shall include visual inspection of signal head operation and comparison to broadcast data
 - Shall include driving through all lanes of intersection at least once to validate MAP data
- On-Site inspection report to be submitted to an SCMS Provider
 - This is just confirmation that inspection was performed – could be an email or a check-box on a portal, submitted by an authorized user representing the DOT
- If SCMS provider does not receive an annual inspection confirmation, provider to contact DOT
- Failure to confirm inspection will cause SCMS Provider to block the RSU

SCMS Manager Intersection Validation Misbehavior Management

SCMS Manager

December 23, 2024

1 Overview

In the context of connected intersection validation, the term *misbehavior* is used to describe a situation where the movement of vehicles is inconsistent with the digitally broadcast intersection state information. For example, cars may drive a path that is not consistent with the approach lanes in the MAP data or stop when the SPaT data indicates a green phase. The proper classification and interpretation of these inconsistencies has been proposed as a core method for performing continuous monitoring of the continued performance of a validated intersection.

These types of inconsistencies can be attributed to several potential causes:

1. Careless or impaired drivers may follow a path that is erratic and inconsistent with the actual lane lines or signal status.
2. Equipment in some vehicles might be misconfigured or faulty, resulting in incorrect BSM data to be broadcast.
3. A local change may override the normal signal and lane indicators, such as a construction or emergency response situation which temporarily alters traffic flow.
4. The digital data that is broadcast may no longer be consistent with the actual lane marking and signal state.

This report considers the impact of misbehavior information provided by the Connected Intersections Message Monitoring System (CIMMS) process. This application collects data broadcast from a connected intersection (in the form of SPaT and MAP data) along with Basic Safety Message (BSM) data from vehicles that drive through the intersection. It then performs analysis to compare the movement of vehicles (as reported in the BSM data) against the intersection status (as indicated in the SPaT and MAP data). Statistical data on misbehavior events is tracked against threshold values.

2 Role of Continuous Monitoring in Intersection Validation

There are several connected vehicle (CV) use cases that depend on accurate and trustworthy broadcast data from intersections. One example application is Red Light Violation Warning (RLVW) which alerts a driver if the on-board safety system determines that they are about to enter an intersection with insufficient time to pass through the intersection before the corresponding signal turns red. Proper operation of this warning requires that the broadcast data representing the signal state and estimated time to the next state transition be timely and accurate.

Experience from early CV system deployments has shown that the level of accuracy and reliability of broadcast data from intersections is difficult to achieve. This has motivated an interest in defining a validation process that compares an intersection system's performance against a defined set of metrics. Systems that achieve the required level of performance against the defined metrics may request special status as *validated* intersections. This status entitles the intersection to broadcast a set of indications that allow vehicles to have confidence in the accuracy and timeliness of the broadcast data.

Experience with previously deployed systems has also demonstrated that intersection performance will change over time. This could be due to configuration changes or software updates to components within the intersection system, or due to physical changes such as road construction that may require changes to the physical lane markings on the ground. Ideally, any change to the intersection system would be immediately followed by changes to the digital data that is broadcast to ensure continued accuracy of the data. However, there are cases where changes may be unplanned or where operational discontinuities may result in situations where broadcast data is not updated.

For this reason, a **continuous monitoring** approach is required to be part of any validated intersection. The goal of monitoring is to quickly detect and respond to any unplanned or unexpected changes in intersection performance that result in data that is out of compliance with validation requirements.

Figure 1 is a state diagram that represents the validation status of an intersection during the operational lifetime of the system. The following sections describe the characteristics of each operating mode along with the transitions between states.

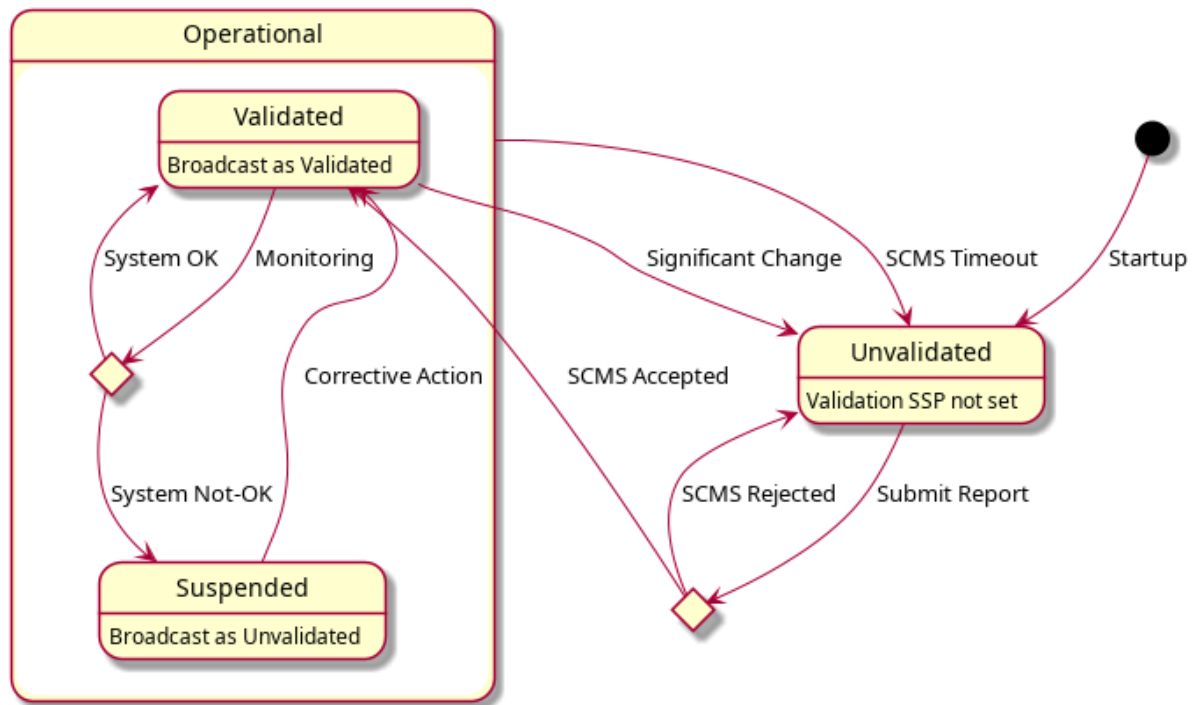


Figure 1: Validation State Diagram

2.1 Unvalidated State

On initial system startup, a newly configured CI starts in an *Unvalidated* state. In this state, the CI may be provided with a production SCMS certificate and it may broadcast signed SPaT, MAP, and RTCM data. However, while the system remains *Unvalidated*, the SCMS Provider will issue application certificates that do not include the SSP bit required to mark the CI as *Validation Enabled*. In this mode, production vehicles may receive and validate the signatures on the CI broadcast data, but vehicles will be aware that the quality of the data is unvalidated.

While in this state, an operator or an authorized contractor may collect data on the performance of the intersection using an approved data collection system. The measurement data collected must account for all operational modes of the intersection. Once data collection is complete, the operator will submit an electronic

report to the corresponding SCMS Provider. This report will identify the intersection and include evaluation results for the initial validation measurements. This step is represented by the *Submit Report* transition.

The SCMS Provider will evaluate the content of the electronic validation report. In some cases, the report may be rejected as shown in the *SCMS Rejected* transition. When this happens, further data collection or corrective actions may be taken by the operator to produce a successful validation report. When the electronic report is accepted, the IC transitions to the *Validated* state via the *SCMS Accepted* transition path.

2.2 Validated State

Once in the *Validated* state, the CI will be issued application certificates that include the SSP bit required to show that the system has been validated. At this point, the continuous monitoring cycle begins. While in this state, SPaT, MAP, RTCM, and BSM data collected at the intersection will be analyzed by the CIMMS application (running locally or as a cloud-hosted service). The *Monitoring* transition shows the conditional evaluation performed by the CIMSS tool. The result of the monitoring activity may confirm that the system is operating within acceptable parameters. In this case the system follows the *System OK* transition back to the *Validated* state.

2.3 Suspended State

If the continuous monitoring detects an anomaly that exceeds a pre-defined threshold, the CI will follow the *System Not-OK* transition to the *Suspended* state. While in this state, the CI must set the application data flag to indicate that the system is not operating in a validated mode. When this bit is not set, production vehicles may receive and validate the signature on the CI data, but it will be aware that the data may not be reliable for some applications, such as RLVW.

In order to recover from the *Suspended* state, the CI operator must take some corrective action. This will require an assessment of the conditions that caused continuous monitoring to determine that the system status is not within acceptable parameters. This may be due to a temporary condition which will self-correct, or it may require minor adjustments to the CI configuration. Once appropriate corrective action has been taken, the operator may instruct the intersection to return to the *Validated* state. At this point, continuous monitoring will resume the role of monitoring the intersection operation. If the problem persists (or if a new problem emerges), then the system will once again transition to the *Suspended* state.

Note that while in the *Validated* state, the operator may execute a planned and managed change to the CI. If this change is deemed to be “significant”, then the operator shall inform the SCMS Provider that a *Significant Change* event has occurred. This will transition the state back to the *Unvalidated* state where it will be issued application certificate with the validation SSP bit cleared. After the planned change is complete, the operator will collect new measurement data using an approved tool and submit a revised validation report to the SCMS provider. This report may be accepted or rejected as with the initial validation report.

At all times while the intersection is in either the *Validated* or *Suspended* state, the SCMS Provider shall monitor the time interval between successive continuous monitoring reports. If the time between reports exceeds a pre-set threshold, the SCMS Provider must cease to issue new application certificates with the validation bit set. This action will force the CI to return to the *Unvalidated* state via the *SCMS Timeout* transition. This transition may happen at any time when the CI is in the *Validated* or *Suspended* state. Recovery from an *SCMS Timeout* will require the submission of an acceptable validation report to the SCMS Provider.

2.4 System Shutdown

At any time, in any state, the system may be shutdown or caused to cease broadcasting CI data. Recovery from a system shutdown will re-start the initial validation process with the system entering the *Unvalidated* state via the *Startup* transition. The shutdown state and corresponding transitions are not shown on in Figure 1 to reduce clutter in the diagram.

3 Event Actions and Recovery

The recommended method for implementing continuous monitoring is through the use of the CIMMS application. This software can be run locally or as a hosted service, using BSM data to report on the movement of vehicles, combined with the broadcast SPaT, MAP, and RTCM messages sent from the connected intersection. The analysis software integrated into CIMMS reports *Events* which indicate anomalies within the data.

CIMMS contains 8 types of event detection algorithms:

1. SPaT/MAP Transmission Rate
2. SPaT/MAP Minimum Data Requirement
3. Signal State Conflict Monitor
4. Time Change Details Monitor
5. Stop Line Passage Event
6. Stop Line Stop Event
7. Direction of Travel
8. Connection of Travel

This set of events can be grouped into two broad categories. The first four reflect directly on the operation of the infrastructure. Events 1 and 2 are triggered if the periodicity or content of the broadcast data is out of specification. Events 3 and 4 are triggered if there is an internal inconsistency in the CI broadcast data, such as overlapping lanes simultaneously showing a green light or significant errors in the signal change time estimate.

Events 5 through 8 reflect on the CI system indirectly. They report information about the movement of vehicles through the intersection and are heavily influenced by the behavior of individual drivers, the configuration of the in-vehicle equipment, and conditions related to the physical lanes and signal head status. Proper interpretation of these events requires further analysis about the expected frequency of outliers and evidence for statistical significance showing that there may be an error in the CI itself.

Note that CIMMS does not currently provide any monitoring for RTCM. Rather than call this out in each section, this point is recognized here only. In a future version, CIMMS shall be updated to include metrics related to RTCM. Current SCMS Manager requirements for intersection validation require that RTCM be present in order for the intersection to achieve *SCMS Accepted* status.

The following sections further discuss the meaning of each event type with a discussion on potential interpretations and actions. Each section describes why an intersection may transition to the *Suspended* state in response to a specific type of event. There is also a definition of the criteria that must be met in order for an operator to attempt to transition the intersection back to the *Validated* state.

3.1 SPaT/MAP Transmission Rate

This event type is triggered when the transmission rate of SPaT or MAP messages deviate from the required 10 messages per-second over a 10 second period. Thresholds within the application put limits on how sensitive this event type is to small changes in message timing. As a direct measure of CI performance, this event type indicates that the system may be unable to maintain a consistent sequence of SPaT or MAP messages. This may be due to CPU load or clock jitter caused by active applications.

Provided that the CIMMS transmission rate filters are set appropriately, occurrences of this event type are expected to be very rare. When this event is triggered, the system shall immediately transition to the *Suspended* state and notify an operator that the system timing needs to be investigated before the CI may be brought back to the *Validated* state.

3.2 SPaT/MAP Minimum Data Requirement

This event type is triggered if the content of one or more SPaT or MAP messages are missing data elements that are marked as critical in the RSU specification. This condition is not expected to occur during normal

operation provided that the CI is configured correctly. As with transmission rate, a CI should transition immediately to the *Suspended* state and notify an operator if this event is triggered. The operator shall perform an investigation into the root cause of the alert before the CI may be brought back to the *Validated* state.

3.3 Signal State Conflict Monitor

A signal state conflict is a condition where multiple lanes are in permissive mode (i.e. green or yellow) simultaneously where those lanes control traffic flows that may cause a collision. This condition should never occur during normal operation. The presence of this alert may indicate a serious failure of the signal controller (a failure that should be prevented by logic in the controller), or a significant discrepancy between the broadcast data and the actual signal head operation.

Both causes potentially present a significant risk to drivers and therefore a CI shall immediately transition to the *Suspended* state and notify an operator if this event occurs. The operator must perform an investigation into the root cause and make corrections before attempting to transition the system back to the *Validated* state.

3.4 Time Change Details Monitor

This event is triggered if there is a significant discrepancy in the predicted time for a future signal change and the timing of evidence that the actual change occurred. For example, a SPaT message may predict 3 seconds to transition from yellow to red but the broadcast may then change to red after only 1 second. This type of discrepancy may occur in rare events where a critical preemption occurs or where there is a shift in timing of messages within the CI system. Thresholds within the CIMMS application are intended to filter out false positive event indications of this type. Only after the pre-configured statistical filters are exceeded shall this event type cause the CI to transition to the *Suspended* state. An operator may attempt to transition the intersection back to the *Validated* state if there is evidence that the root cause has been eliminated.

3.5 Stop Line Passage Event

This event type is recorded every time a vehicle crosses a stop line in an MAP approach while adhering to certain parameters on speed and direction. Only if internal thresholds are crossed will this event trigger a notification indicating that there may be a timing issue.

A notification of this type indicates that multiple stop line passage events happened when the broadcast SPaT data indicated that the lane should be stopped. This may be due to a significant disparity in timing between the SPaT message broadcast and the actual signal head.

An occurrence of a notification of this type, after processing by the internal CIMMS statistical filters, shall result in the intersection transitioning to the *Suspended* state with a notification to the operator. An operator must review the collection of vehicle data that caused the notification and resolve any common cause issues prior to attempting to transition the CI back to the *Validated* state. If the operator determines that there is no significant deviation between the CI broadcast data and the actual intersection status, then it is permissible to adjust the CI thresholds to reduce the likelihood of future false positive notifications.

3.6 Stop Line Stop Event

This event type is recorded every time a vehicle is stopped at a stop line in a MAP approach lane while the SPaT data indicates that the corresponding lane should be in a permissive mode (green or yellow). The internal thresholds in the CIMMS application should filter out normal driver delays. Any resulting notification may indicate a disparity in the broadcast SPaT data and the actual signal head action.

An occurrence of a notification of this type, after processing by the internal CIMMS statistical filters, shall result in the intersection transitioning to the *Suspended* state with a notification to the operator. An operator must review the collection of vehicle data that caused the notification and resolve any common cause issues prior to attempting to transition the CI back to the *Validated* state. If the operator determines that there is

no significant deviation between the CI broadcast data and the actual intersection status, then it is permissible to adjust the CI thresholds to reduce the likelihood of future false positive notifications.

3.7 Direction of Travel

This event type aggregates movement data across multiple vehicles as they pass through an intersection. Based on thresholds set in the CIMMS application, a notification of this type may be generated to indicate that a significant number of vehicles are moving in a direction that is inconsistent with the broadcast MAP data. This could indicate that the MAP data is no longer aligned with the actual lane lines, or that there is some other condition causing traffic to change route. The root cause may be related to an temporary event such as an accident, emergency vehicle activity, or a change in road conditions (such as flooding, ice, hole in the roadway, etc). However, this notification may also indicate that the MAP data that is being broadcast is no longer consistent with the normal flow of traffic. If the MAP data is systematically shifted it may cause the CIMMS system to place some cars in a different lane than the one where they are actually driving. This condition would likely result in vehicles having similar difficulty in correctly identifying their lane of travel and therefore hinder their ability issue reliable alerts to drivers.

3.8 Connection of Travel

Similar to direction of travel, this event type aggregates the movement of multiple vehicles through an intersection. A notification of this type is generated only if internal thresholds are exceeded over a defined period of time. The notification indicates that multiple vehicles have traversed lanes in a way that is not permitted in the MAP data. For example, multiple cars may be proceeding straight from a turn-only lane. A few isolated incidents of this type may be attributed to careless or distracted drivers who fail to follow the posted lane restrictions. When multiple vehicles follow a similar unauthorized path it may indicate a significant error in the MAP data, or a temporary condition that is causing traffic to move in an unexpected way through the intersection.

4 Defining Event Thresholds

Many of the event types defined in the prior section depend on internal statistical thresholds in the CIMMS system. In setting these thresholds, it is valuable to consider the factors that impact the statistical significance of several event types. This analysis supports the development of a spreadsheet model that can be used to support the bounds on thresholds that shall be used when configuring a CIMMS system. At this time, this section is intended to be informative and not declarative. Over time and with validation experience, it is expected that SCMS Manager will publish more specific guidance on threshold values.

This guidance is specifically intended for use with the indirect event types that may be triggered by CIMMS. The four indirect types include “Stop Line Passage Event”, “Stop Line Stop Event”, “Direction of Travel”, and “Connection of Travel”. Each of these events may be significantly impacted by a combination of factors that include driver behavior, vehicle system configuration, short-term disturbances, and CI configuration errors. In most cases, it is not possible to distinguish among these distinct causes based only on the BSM and CI data captured by the CIMSS system. However, with appropriate modeling, it may be possible to anticipate an acceptable rate for type 1 errors (false positives) and type 2 errors (false negatives). The following sections describe an approach that may be useful in modeling driver behavior and placing bounds on these error types. Over time, actual vehicle data may be used to define specific distribution parameters to produce actionable threshold settings.

4.1 Modeling Driver Behavior

Human drivers will never follow a perfect path or have perfect reaction times. There will always be significant variation among drivers that will impact their driving patterns including bias to one side of a lane or the other, stopping distance with respect to a stop line, and reaction times. Even a single driver will never perfectly

repeat a particular driving pattern. When averaging among a large number of drivers, it is reasonable to assume that driver metrics can be modeled using a Normal distribution.

The following method can be used to estimate the expected number of violations that may be observed per-day. In the specific example, stop location violations are considered. A similar methodology can be used to estimate frequency of occurrence for other parameters.

- Assume that the number of vehicles that arrive at a specific lane at a specific intersection can be modeled using a Poisson distribution with parameter λ set to the observed mean number of vehicles per-day observed over a period of time.
- Assume that the actual location where a driver stops with respect to the stop line can be modeled using a Normal distribution with a mean μ and standard deviation σ .
- Define a *critical distance* D as a distance beyond the stop line that causes significant threat to the flow of traffic.

Based on these parameters, perform the following calculations:

- The Z-Score for the Normal distribution is calculated as $Z = \frac{D-\mu}{\sigma}$
- The probability of a violation is $p = 1 - s(Z)$ where $s()$ is the standard Cumulative Distribution Function (CDF) of the Normal distribution. This estimates the probability p that any one vehicle will exceed the *critical distance*, D .
- Estimate the number of expected daily violations as $N = \lambda * p$

A spreadsheet model is included that performs these calculations. For example, with $\lambda = 1,200$ vehicles per-day, $\mu = -0.5$ meters, standard deviation $\sigma = 0.8$ meters, and a critical distance $D = 0.7$ meters, the expected number of violations is 81 per-day. Using this model, with actual data collected from real driver metrics and vehicle arrival rates, can provide critical guidance for thresholds used in configuring the CIMSS detection algorithms.

Note that the assumption of a Normal distribution for stop distance must be validated with a test of fit for the Normal distribution. Similarly, the use of a Poisson distribution to approximate vehicles per-day per-lane must be validated using data. It is possible that the vehicle stopping distance is biased to one side, indicating that an exponential distribution may be a better fit. Also, the arrival rate of vehicles likely changes by season, so the parameters may need to be adjusted based on season.

4.2 Extension to Other Parameters

The modeling approach described in the previous section may be extended to set expected values for other properties such as calculating the probability of classifying a vehicle in the wrong lane, resulting in a direction of travel or connection of travel violation. With sufficient data collected from actual vehicles, it will be possible to estimate the actual sensitivity of the CIMMS method can be estimated for specific measurements such as lane line accuracy, stop line accuracy, and SPaT phase timing.



CI Test Results Report Format
Version 0.8

Amit Kapoor
05-31-2024

Contents

1	Abstract	3
2	Status of This Standard	3
3	Introduction	4
3.1	Terminology	5
4	Report Requirements	7
4.1	Machine-Readable Format	7
5	Implementation Strategy	8
6	Introduction to OSCAL	10
6.1	What is OSCAL?	10
6.2	Key Objectives	10
6.2.1	Standardization	10
6.2.2	Automation	10
6.2.3	Consistency	10
6.3	OSCAL Layers and Models	10
6.3.1	Control Layer	10
6.3.2	Implementation Layer	11
6.3.3	Assessment Layer	11
6.4	Benefits of OSCAL	11
6.4.1	Improved Efficiency	11
6.4.2	Enhanced Interoperability	11
6.4.3	Better Risk Management	11
6.4.4	Scalability	11
6.5	Summary	11
7	OSCAL Assessment Report Format	12
7.1	Assessment Results Organization	12
7.2	OSCAL Assessment Report Example	13
8	Summary	19
8.1	Standardization and Interoperability	19
8.2	Automation and Efficiency	19
8.3	Enhanced Risk Management	19
8.4	Facilitating Continuous Monitoring	19
8.5	Conclusion	19
	Bibliography	20

1 Abstract

This report, as part of the Utah Smartgrant initiative, outlines a recommended format for traffic organizations to use when providing cybersecurity test results for connected intersections to Security Credential Management System (SCMS) providers. This machine-readable format is crucial for maintaining accurate and up-to-date cybersecurity information throughout the lifecycle of the connected intersection. By adopting this standardized format, SCMS providers can automate the certification process, ensuring continuous compliance and security monitoring, and enhancing the overall efficiency and effectiveness of the cybersecurity management for connected intersections.

2 Status of This Standard

This is a standard being proposed by SCMS Manager for all IOOs and SCMS providers under the Utah Smart Grant project.

3 Introduction

The integration of Secure Credential Management System (SCMS) in connected intersections is critical to ensuring secure and reliable communication within the Vehicle-to-Everything (V2X) ecosystem. SCMS providers play a crucial role in issuing and managing digital certificates that authenticate V2X messages, ensuring the integrity, authenticity, and confidentiality of data exchanges between vehicles, infrastructure, and other entities. These certificates are essential for building trust in the V2X network, preventing malicious actors from injecting false data, and maintaining the overall safety and efficiency of traffic systems. Certificates are issued to various components and parties in the ecosystem, such as vehicles, roadside units, and infrastructure elements, ensuring that each entity in the network can be reliably authenticated.

To maintain a high level of security and operational efficiency, SCMS providers require detailed technical reports from each connected intersection reflecting implementation of various cybersecurity controls. These reports must confirm that intersections are functioning correctly, adhering to mandated security protocols, and capable of securely managing the digital certificates issued by the SCMS provider. The reports will enable SCMS providers to issue initial certificates and continue renewing them, ensuring that only compliant and secure intersections remain part of the V2X network. For streamlined processing and integration into existing systems, these reports must be in a machine-readable format, allowing for automated analysis and quick decision-making.

3.1 Terminology

- **V2X (Vehicle-to-Everything):** A communication technology that enables vehicles to interact with other vehicles (V2V), infrastructure (V2I), pedestrians (V2P), and networks (V2N) to enhance traffic safety, efficiency, and convenience.
- **SCMS (Secure Credential Management System):** A system that manages digital certificates used to authenticate V2X messages, ensuring the integrity, authenticity, and confidentiality of communications within the V2X ecosystem.
- **Digital Certificates:** Electronic documents used to verify the identity of entities (vehicles, infrastructure) within the V2X network. Issued by the SCMS, these certificates ensure secure communication by providing cryptographic proof of identity.
- **Cryptographic Keys:** Secure digital codes used in cryptographic algorithms to encrypt and decrypt data, ensuring the confidentiality and integrity of communications within the V2X system.
- **JSON (JavaScript Object Notation):** A lightweight, text-based data interchange format that is easy for humans to read and write and easy for machines to parse and generate. Commonly used for transmitting data in web applications.
- **XML (eXtensible Markup Language):** A markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. Often used in enterprise systems for data interchange.
- **Protobuf (Protocol Buffers):** A method developed by Google for serializing structured data, more efficient in terms of performance and space compared to JSON and XML. Used for transmitting data across network services.
- **Latency:** The time taken for a message to travel from its source to its destination in a network. Low latency is crucial for real-time V2X communications to ensure timely and accurate information exchange.
- **Throughput:** The amount of data successfully transmitted from one place to another in a given amount of time. High throughput is essential for handling the large volume of data in V2X communications.
- **Certificate Revocation:** The process of invalidating a previously issued digital certificate before its scheduled expiration date. This is done if the certificate is compromised or no longer trusted.
- **Key Management:** The process of handling cryptographic keys, including their generation, exchange, storage, use, and replacement. Proper key management is vital for maintaining the security of V2X communications.
- **Interference:** Disruptions in communication signals caused by external factors such as physical obstacles, other electronic devices, or environmental conditions. Minimizing interference is essential for reliable V2X communications.
- **Anomaly Detection:** The process of identifying unusual patterns or behaviors in data that do not conform to expected norms. In V2X systems, anomaly detection helps in identifying potential security breaches or operational issues.
- **Machine-Readable Format:** Data formats that are easily processed by computers, enabling automated systems to read, interpret, and act on the data without human intervention. Common formats include JSON, XML, and Protobuf.
- **Encryption Protocols:** Algorithms and standards used to encrypt data, ensuring its confidentiality and integrity during transmission. Common protocols include AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman).
- **Incident Response:** The actions taken by an organization to address and manage the aftermath of a security breach or cyberattack. Effective incident response is critical for minimizing damage and restoring normal operations in V2X systems.

- OSCAL (Open Security Controls Assessment Language): A set of standardized, machine-readable formats (XML, JSON, YAML) developed by NIST to enhance the efficiency and consistency of security control assessments.

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in (Bradner 1997).

4 Report Requirements

1. Operational Status

- *Health Check*: Includes information about the intersection's operational status, such as uptime, system diagnostics, and any detected anomalies.
- *Sensor and Device Status*: Details the status of all connected sensors and devices, including their operational state, firmware versions, and any fault reports.
- *Data Integrity Checks*: Ensures the data being transmitted by the intersection's systems is accurate and untampered.
- *Message Logs*: Logs of V2X messages sent and received, including timestamps, message types, and any errors encountered.
- *Latency and Throughput Metrics*: Performance metrics for message transmission, including average and peak latency, and data throughput.
- *Interference Reports*: Reports on any detected interference or disruptions in communication channels.

2. Security Compliance

- *Certificate Status*: Provides details on the current status of all certificates used by the intersection, including expiration dates and any revocations.
- *Key Management*: Information on key generation, storage, and usage policies, including audit logs of key usage.
- *Incident Reports*: Logs of any security incidents, such as attempted breaches, detected intrusions, and responses to these incidents.
- *Encryption Protocols*: Details on the encryption standards and protocols in use, including any updates or changes made.

4.1 Machine-Readable Format

To ensure that these reports can be automatically processed by SCMS providers, they must be delivered in a machine-readable format. This can be achieved through standardized data formats such as JSON, XML, YAML, or Protocol Buffers (Protobuf). The choice of format will depend on the specific requirements of the SCMS provider and the existing infrastructure of the connected intersections. However, in this report, there will be a recommendation for a canonical format.

- **JSON (JavaScript Object Notation)**: A lightweight data-interchange format that is easy to read and write for humans and machines. Ideal for systems with a preference for web-based technologies.
- **XML (eXtensible Markup Language)**: A markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. Commonly used in enterprise applications.
- **Protocol Buffers (Protobuf)**: A method developed by Google for serializing structured data, more efficient in terms of performance and space compared to JSON and XML.
- **YAML (YAML Ain't Markup Language)**: YAML is a human-readable data serialization standard that is commonly used for configuration files and data exchange between languages with different data structures. It is designed to be simple and easy to read, making it ideal for developers and system administrators.

5 Implementation Strategy

- **Report Schemas:** Develop comprehensive report format ensuring all necessary information is included and correctly formatted.
- **Automated Report Generation:** Implement systems at each intersection that can automatically generate the required reports at specified intervals or upon specific triggers.
- **Secure Transmission:** Ensure the secure transmission of reports from intersections to the SCMS provider, using encryption protocols to protect the data in transit.
- **Validation and Auditing:** Develop mechanisms for the SCMS provider to validate the received reports, checking for completeness, accuracy, and compliance with security standards.
- **Feedback Loop:** Establish a feedback loop where the SCMS provider can notify intersections of any issues detected in the reports, prompting corrective actions.
- **CI Lifecycle:** Supporting a Connected Intersection (CI) through its full lifecycle for security certification involves continuous monitoring, regular assessments, and periodic updates to ensure compliance with security standards, the effectiveness of implemented controls, and the issuance and management of necessary digital certificates to maintain secure operations.

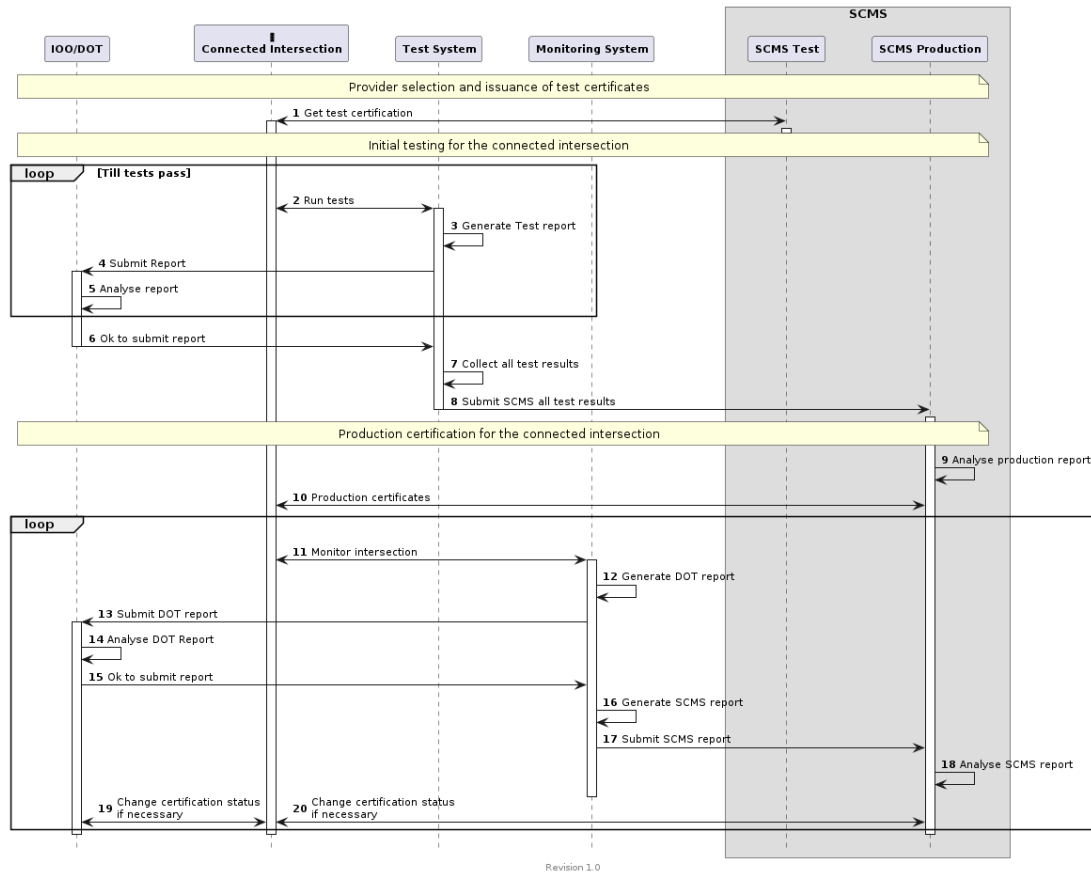


Figure 1: Report Flows

When implementing a cybersecurity assessment report for connected intersections, it is highly recommended to adopt an already established format rather than designing a new custom one. Using a pre-existing format offers several advantages:

- **Standardization:** Leveraging a widely recognized format ensures consistency and compatibility across various systems and organizations.

- **Interoperability:** Existing formats are designed to work seamlessly with different tools and platforms, facilitating smoother integration and data exchange.
- **Proven Reliability:** Established formats have undergone extensive testing and validation, minimizing the risk of errors and issues.
- **Efficiency:** Implementing a pre-existing format reduces development time and effort, allowing organizations to focus on other critical aspects of the cybersecurity assessment process.

By choosing a well-supported and widely accepted format, organizations can ensure robust, efficient, and secure reporting mechanisms that align with industry best practices.

6 Introduction to OSCAL

6.1 What is OSCAL?

The Open Security Controls Assessment Language (**OSCAL**) is a set of hierarchical, structured formats expressed in XML, JSON, and YAML. Developed by the **National Institute of Standards and Technology (NIST)**, OSCAL standardizes the representation of information in information security, particularly for security controls, assessments, and continuous monitoring. The goal is to facilitate automation, improve efficiency, and ensure consistency in managing security controls across various frameworks and organizations.

6.2 Key Objectives

6.2.1 Standardization

OSCAL provides a common language for expressing security controls, assessments, and related information, reducing complexity and improving interoperability between different systems and tools.

6.2.2 Automation

With **machine-readable formats**, OSCAL supports the automation of security assessment processes, significantly reducing the time and effort required for compliance checks, risk assessments, and continuous monitoring.

6.2.3 Consistency

Using OSCAL ensures that security control information is consistent across different frameworks and organizations, which is crucial for effective risk management and meeting regulatory requirements.

6.3 OSCAL Layers and Models

OSCAL is organized into three main layers, each consisting of one or more models that address specific aspects of security controls and assessments.

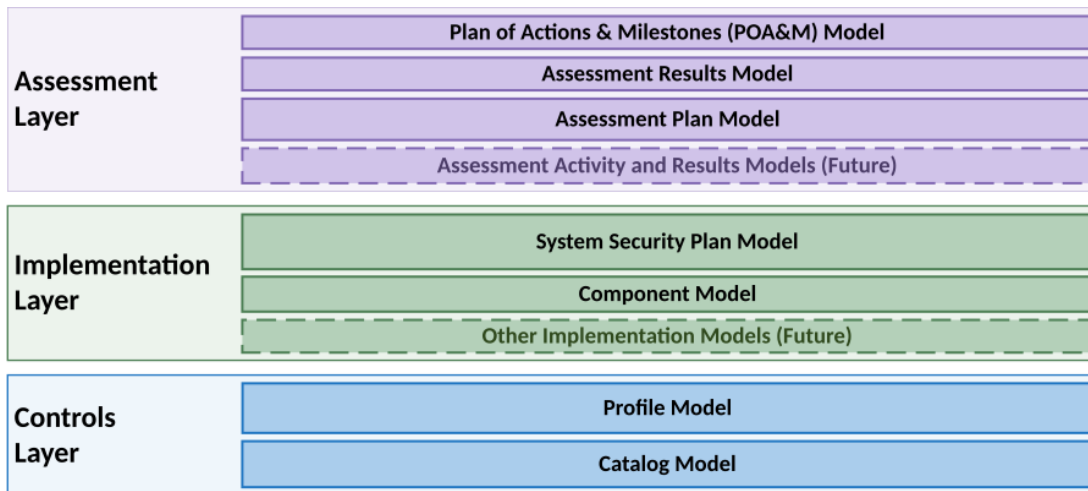


Figure 2: OSCAL Layers

6.3.1 Control Layer

The Control Layer focuses on the representation and organization of security controls. It includes:

- **Catalog Model:** Organizes security controls into a catalog, supporting various frameworks.

- **Profile Model:** Enables the selection and tailoring of controls to create a specific set, known as a profile.

6.3.2 Implementation Layer

The Implementation Layer addresses how security controls are implemented within a system. It includes:

- **System Security Plan (SSP) Model:** Describes how security controls are implemented within an information system.
- **Component Definition Model:** Defines individual components that can satisfy controls, such as policies, processes, hardware, software, or services.

6.3.3 Assessment Layer

The Assessment Layer focuses on assessing the implementation and effectiveness of security controls. It includes:

- **Assessment Plan Model:** Outlines the plan for conducting security assessments.
- **Assessment Results Model:** Captures the results of security assessments, including findings, evidence, and observations.
- **Plan of Action and Milestones (POA&M) Model:** Tracks the remediation of identified issues.

6.4 Benefits of OSCAL

6.4.1 Improved Efficiency

Standardizing and automating security control assessments significantly reduces the time and effort required for compliance and risk management activities.

6.4.2 Enhanced Interoperability

OSCAL's machine-readable formats facilitate the exchange of information between different systems and tools, improving interoperability and reducing the risk of errors.

6.4.3 Better Risk Management

Consistent and accurate representation of security controls helps organizations manage risks more effectively, ensuring compliance with regulatory requirements and protection of their information systems.

6.4.4 Scalability

OSCAL's structured formats and support for automation make it easier to scale security assessments and continuous monitoring across large and complex environments.

6.5 Summary

OSCAL represents a significant advancement in the standardization and automation of security controls assessment and management. By adopting OSCAL, organizations can improve the efficiency, consistency, and effectiveness of their security programs, enhancing their ability to manage risks and comply with regulatory requirements. As OSCAL continues to evolve, it is poised to play a critical role in the future of cybersecurity management.

For more detailed information and updates on OSCAL, visit the NIST OSCAL website.

7 OSCAL Assessment Report Format

The OSCAL Assessment Results model defines the information contained within an assessment report supporting assessment and continuous monitoring capabilities. The OSCAL Assessment Results model is part of the OSCAL Assessment Layer. It defines structured, machine-readable XML, JSON, and YAML representations of the information contained within an assessment report.

This model is typically used by anyone performing assessment or continuous monitoring activities on a system to determine the degree to which that system complies with one or more frameworks.

This model allows an assessor to express all details associated with a classic “snapshot in time” assessment, including the scope of the assessment, times and dates of activities, actual assessment activities performed, as well as any observations, findings, and identified risks. It also allows organizations to report continuous assessment information.

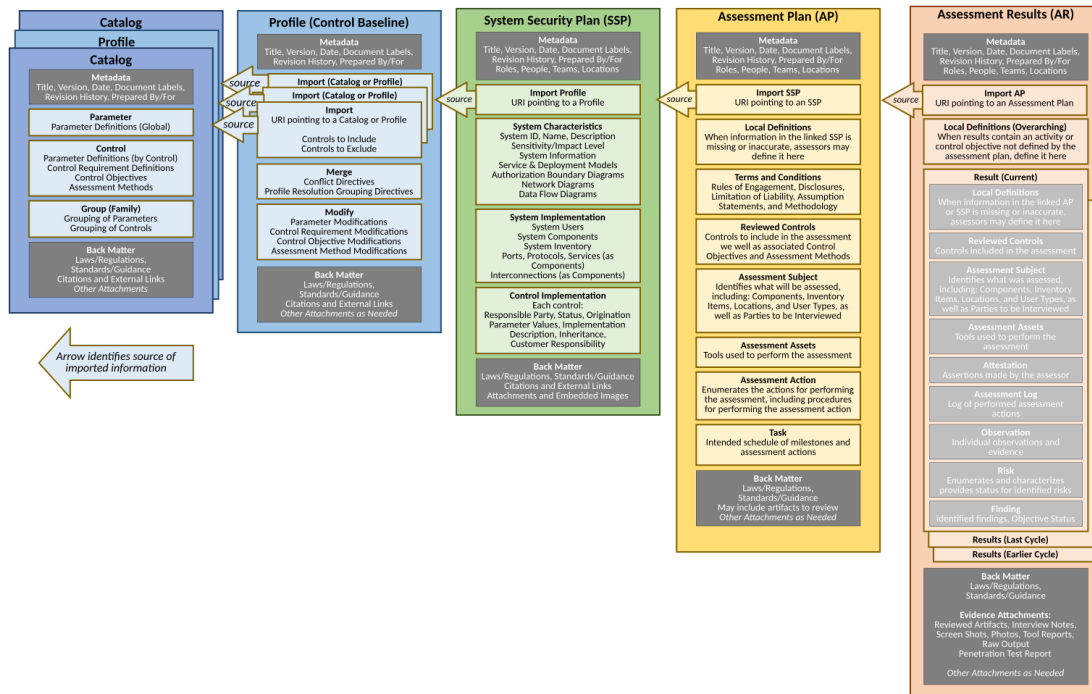


Figure 3: OSCAL Assessment Report

7.1 Assessment Results Organization

An OSCAL assessment report is organized as follows:

- **Metadata:** Metadata syntax is identical and required in all OSCAL models. It includes information such as the file’s title, publication version, publication date, and OSCAL version. Metadata is also used to define roles, parties (people, teams and organizations), and locations.
- **Import AP:** Identifies the OSCAL-based assessment plan (AP) for this assessment. The AP imports several pieces of information about the system being assessed including the system security plan (SSP), which is also represented according to the OSCAL SSP model. This linking of data eliminates the need to duplicate and maintain the same information in multiple places.
- **Local Definitions:** When the assessment results contain an activity or control objective not defined by the assessment plan, assessors define it here instead.
- **Results:** Describes the assessment findings, identified risks, and recommended remediation. Also identifies false positive results, risk adjustments, and operationally required risks, as well as when the results should expire.

- Local Definitions: Normally other aspects of the assessment results point to content in the linked Assessment Plan and SSP. When the AR must reference information that is missing from the linked AP or SSP, assessors define it here instead.
- Reviewed Controls: Identifies the controls actually reviewed by this assessment.
- Assessment Subject: Identifies the in-scope elements of the system, including locations, components, inventory items, and users.
- Assessment Assets: Identifies the assessor’s assets used to perform the assessment, including the team, tool, and rules of engagement content.
- Attestation: Assertions made by the assessor.
- Assessment Log: Log of performed assessment actions. This includes start and end timestamps for individual actions performed by the assessment team, with an optional link to defined assessment actions.
- Observation: Individual observations and related evidence. This may be evidence of compliance or non-compliance.
- Risk: Identifies individual risks, including weakness description, risk statement, and other risk characteristics.
- Finding: Identifies findings resulting from observations and risks, and can include the control objective status.
- **Back Matter:** Back matter syntax is identical in all OSCAL models. It is used for attachments, citations, and embedded content such as graphics.

7.2 OSCAL Assessment Report Example

```
{
  "assessment-results": {
    "uuid": "ec0dad37-54e0-40fd-a925-6d0bdea94c0d",
    "metadata": {
      "title": "IFA GoodRead Continuous Monitoring Assessment Results June 2023",
      "last-modified": "2024-02-01T13:57:28.355446-04:00",
      "version": "202306-002",
      "oscal-version": "1.1.2",
      "roles": [
        {
          "id": "assessor",
          "title": "IFA Security Controls Assessor"
        }
      ],
      "parties": [
        {
          "uuid": "e7730080-71ce-4b20-bec4-84f33136fd58",
          "type": "person",
          "name": "Amy Assessor",
          "member-of-organizations": [
            "3a675986-b4ff-4030-b178-e953c2e55d64"
          ]
        },
        {
          "uuid": "3a675986-b4ff-4030-b178-e953c2e55d64",
          "type": "organization",
          "name": "Important Federal Agency",
          "short-name": "IFA",
          "links": [
            {
              "href": "https://www.ifa.gov",
              "rel": "website"
            }
          ]
        }
      ]
    }
  }
}
```

```

    }
  ]
}
],
"responsible-parties": [
  {
    "role-id": "assessor",
    "party-uuids": [
      "e7730080-71ce-4b20-bec4-84f33136fd58"
    ]
  }
]
],
"import-ap": {
  "href": "../ap.oscal.xml"
},
"local-definitions": {
  "activities": [
    {
      "uuid": "cf5d53fe-6043-4c68-9ed6-6b258909febf",
      "title": "Test System Elements for Least Privilege Design and Implementation",
      "description": "The activity and it steps will be performed by the assessor via their security automation platform to test least privilege design and implementation of the system's elements, specifically the cloud account infrastructure, as part of continuous monitoring.",
      "props": [
        {
          "name": "method",
          "value": "TEST"
        }
      ],
      "steps": [
        {
          "uuid": "57f8cfb8-fc3f-41d3-b938-6ab421c92574",
          "title": "Configure Cross-Account IAM Role Trust for GoodRead and Assessor AwesomeCloud Accounts",
          "description": "The GoodRead system engineer will coordinate with the assessor's engineering support staff to configure an IAM role trust. A service account for automation with its own role with the assessor's AwesomeCloud account can assume the role for read-only assessor operations within the GoodRead Product Team's AwesomeCloud account for continuous monitoring of least privilege.",
          "remarks": "This step is complete.\n\nGoodRead Product Team and SCA Engineering Support configured the latter's cross-account role trust and authentication and authorization in to the former's account on May 29, 2023."
        },
        {
          "uuid": "976aadad-b1ce-475b-aa6c-e082537e7902",
          "title": "Automate Cross-Account Login to GoodRead AwesomeCloud Account",
          "description": "The assessor's security automation platform will create a session from their dedicated will obtain access to the

```

```

    GoodRead Product Team's AwesomeCloud account with their single
    sign-on credentials to a read-only assessor role.",
    "remarks": "This step is complete.\n\nGoodRead Product Team and
    SCA Engineering Support tested scripts from the security
    automation platform interactively on May 30, 2023, to confirm
    they work ahead of June 2023 continuous monitoring cycle."
  },
  {
    "uuid": "18ce4e19-7432-4484-8e75-2dd8f05668cf",
    "title": "Analyze GoodRead Developer and System Engineer Roles
    for Least Privilege",
    "description": "Once authenticated and authorized with a
    cross-account session, the security automation pipeline will
    execute scripts developed and maintained by the assessor's
    engineering support staff. It will analyze the permitted actions
    for the developer and system engineer roles in the GoodRead
    Product Team's AwesomeCloud account to confirm they are designed
    and implement to facilitate only least privilege operation.
    Examples are included below.\n\n* For the GoodRead developer role
    in their AwesomeCloud account, the developer role may only permit
    the user with this role to check the IP addresses and status of
    the Awesome Compute Service server instances. This role will not
    permit the user to create, change, or delete the instances.
    Similarly, the developer will permit a user to perform actions to
    see IP addresses of an Awesome Load Balancer instance, but not
    add, change, or delete the instances.\n* For the GoodRead system
    engineer role in their AwesomeCloud account, the system engineer
    role may only permit actions where the user can add, change, or
    delete instances for approved services (i.e. Awesome Compute
    Service, Awesome Load Balancer, et cetera). The role may not
    permit actions by the user for any other service.\n"
  }
],
"related-controls": {
  "control-selections": [
    {
      "include-controls": [
        {
          "control-id": "ac-6.1"
        }
      ]
    }
  ]
},
"responsible-roles": [
  {
    "role-id": "assessor",
    "party-uuids": [
      "e7730080-71ce-4b20-bec4-84f33136fd58"
    ]
  }
]
},
]
},
},

```

```

"results": [
  {
    "uuid": "ald20136-37e0-42aa-9834-4e9d8c36d798",
    "title": "IFA GoodRead Continous Monitoring Results June 2023",
    "description": "Automated monthly continuous monitoring of the GoodRead information system's cloud infrastructure recorded observations below. Additionally, contingent upon the confidence level of the observations and possible risks, confirmed findings may be opened.",
    "start": "2023-06-02T08:31:20-04:00",
    "end": "2023-06-02T08:46:51-04:00",
    "local-definitions": {
      "tasks": [
        {
          "uuid": "35876484-aa4b-494d-95a2-0d1cc04eb47e",
          "type": "action",
          "title": "Test System Elements for Least Privilege Design and Implementation",
          "description": "The activity and it steps will be performed by the assessor via their security automation platform to test least privilege design and implementation of the system's elements, specifically the cloud account infrastructure, as part of continuous monitoring.",
          "associated-activities": [
            {
              "activity-uuid": "cf5d53fe-6043-4c68-9ed6-6b258909febf",
              "subjects": [
                {
                  "type": "component",
                  "include-all": {}
                }
              ]
            }
          ]
        }
      ]
    }
  },
  "reviewed-controls": {
    "control-selections": [
      {
        "include-controls": [
          {
            "control-id": "ac-6.1"
          }
        ]
      }
    ]
  },
  "observations": [
    {
      "uuid": "8807eb6e-0c05-43bc-8438-799739615e34",
      "title": "AwesomeCloud IAM Roles Test - GoodRead System Engineer Role",
      "description": "Test AwesomeCloud IAM Roles for least privilege design and implementation.",
      "methods": [
        "TEST"
      ]
    }
  ]
}

```

```

    ],
    "types": [
      "finding"
    ],
    "subjects": [
      {
        "subject-uuid": "551b9706-d6a4-4d25-8207-f2ccec548b89",
        "type": "component"
      }
    ],
    "collected": "2023-06-02T08:31:20-04:00",
    "expires": "2023-07-01T00:00:00-04:00",
    "remarks": "The assessor's security automation platform analyzed all roles specific to the GoodRead Product Team, not those managed by the Office of Information Technology. The `IFA-GoodRead-SystemEngineer` role in their respective AwesomeCloud account permitted use of the following high-risk actions.\n\n* awesomecloud:auditlog>DeleteAccountAuditLog\n* awesomecloud:secmon:AdministerConfigurations\n\nBoth of these actions are overly permissive and not appropriate for the business function of the staff member assigned this role."
  },
  {
    "uuid": "4a2fb32e-9be9-43cf-b717-e9e47de061bd",
    "title": "AwesomeCloud IAM Roles Test - GoodRead Developer Role",
    "description": "Test AwesomeCloud IAM Roles for least privilege design and implementation.",
    "methods": [
      "TEST"
    ],
    "types": [
      "finding"
    ],
    "subjects": [
      {
        "subject-uuid": "551b9706-d6a4-4d25-8207-f2ccec548b89",
        "type": "component"
      }
    ],
    "collected": "2023-06-02T08:31:20-04:00",
    "expires": "2023-07-01T00:00:00-04:00",
    "remarks": "The assessor's security automation platform detected that the developer's role is permitted to perform only permissible actions in the GoodRead AwesomeCloud account in accordance with the agency's least privilege policy and procedures."
  }
],
"risks": [
  {
    "uuid": "0cfa750e-3553-47ba-a7ba-cf84a884d261",
    "title": "GoodRead System Engineers Have Over-Privileged Access to Cloud Infrastructure",
    "description": "A user in the GoodRead cloud environment with the privileges of a system engineer can exceed the intended privileges for their related business function. They can delete all historical audit records and remove important security monitoring functions

```

```
for the IFA Security Operations Center staff.",
"statement": "An account without proper least privilege design and implementation can be used to surreptitiously add, change, or delete cloud infrastructure to the too managing all links to IFA's communication to public citizens, potentially causing significant harm with no forensic evidence to recover the system. Regardless of the extent and duration of a potential incident, such a configuration greatly increases the risk of an insider threat if there were likely to a potential insider threat in the GoodRead Product Team.\n\nIf such an insider threat existed and acted with this misconfiguratio, the resulting event could cause significant financial and reputational risk to IFA's Administrator, executive staff, and the agency overall.",
"status": "investigating"
}
],
"findings": [
{
"uuid": "45d8a6c2-1368-4bad-9ba0-7141f0a32889",
"title": "GoodRead AwesomeCloud Account's System Engineer Role Permits High Risk Actions",
"description": "The assessor's security automation platform detected that the system engineer's role is permitted to perform the following actions in the GoodRead AwesomeCloud account.\n\n* Delete and reset account audit logs.\n* Add, change, or delete security monitoring configurations in the Awesome Security Monitor service used by the IFA Security Operations Center.\n\n\nThe system engineer is not permitted to modify these services and their role was incorrectly configured.",
"target": {
"type": "objective-id",
"target-id": "ac-6.1_obj",
"description": "This is a finding.",
"status": {
"state": "not-satisfied"
}
}
},
"implementation-statement-uuid": "d5f9b263-965d-440b-99e7-77f5df670a11",
"related-observations": [
{
"observation-uuid": "8807eb6e-0c05-43bc-8438-799739615e34"
}
],
"related-risks": [
{
"risk-uuid": "0cfa750e-3553-47ba-a7ba-cf84a884d261"
}
]
}
]
}
```

8 Summary

8.1 Standardization and Interoperability

The OSCAL (Open Security Controls Assessment Language) assessment report format provides a standardized, machine-readable way to convey cybersecurity assessment results. By adhering to a common structure and format, organizations can ensure consistency in how security information is reported, making it easier to compare and integrate data across different systems and frameworks. This standardization promotes interoperability, allowing various tools and systems to seamlessly exchange and process security assessment data.

8.2 Automation and Efficiency

One of the key advantages of using the OSCAL assessment report format is the ability to automate the generation, validation, and processing of security assessment reports. Automation reduces the manual effort required to compile and analyze assessment data, thus increasing efficiency and accuracy. With OSCAL, organizations can leverage automated tools to streamline the assessment process, quickly identify compliance gaps, and generate comprehensive reports without the risk of human error.

8.3 Enhanced Risk Management

The OSCAL assessment report format supports detailed and structured documentation of security controls and their assessment results. This structured approach helps organizations maintain a clear and comprehensive view of their security posture, facilitating better risk management. By providing a transparent and consistent way to report on security controls, OSCAL enables organizations to more effectively monitor and manage risks, ensuring that security measures are adequately implemented and maintained.

8.4 Facilitating Continuous Monitoring

In the rapidly evolving cybersecurity landscape, continuous monitoring is crucial for maintaining a robust security posture. The OSCAL assessment report format supports ongoing assessment and monitoring activities by providing a consistent and repeatable method for documenting and reporting security control assessments. This capability allows organizations to maintain up-to-date security information, quickly respond to emerging threats, and ensure continuous compliance with regulatory requirements.

8.5 Conclusion

The OSCAL assessment report format offers significant benefits in terms of standardization, automation, risk management, and continuous monitoring. By adopting OSCAL, organizations can improve the efficiency and effectiveness of their cybersecurity assessments, ensuring that they can quickly adapt to changing security landscapes and maintain robust protection for their information systems.

Bibliography

Bradner, Scott. 1997. “Key Words for Use in Rfcs to Indicate Requirement Levels.” BCP 14. RFC Editor; Internet Requests for Comments; RFC Editor. <http://www.rfc-editor.org/rfc/rfc2119.txt>.



CTI4501 Security Policy Profile

Amit Kapoor

August 20, 2024
Version 1.0

Contents

Background	4
Expansion of Security Requirements	4
Applicability to Connected Intersection Authorities	4
Focused Scope of RSU-Specific Requirements	4
Risk-Driven Requirements and Mitigation Policies	4
Subset CTI4501 Security Requirements	5
Document Structure	6
Data Trustworthiness: Sources and Processing	7
Integrity of Operations for Internal CI Data Entities	7
Events to be Monitored by Self-Monitoring	7
Protect V2X Radio Parameters	8
Intersection Identifier Trustworthiness	9
Robustness of Intersection Identifier Assignment	9
Detect Incorrect Intersection Identifiers	10
Manage Incorrect Intersection Identifiers	10
Detect Duplicate Use of Intersection Identifiers by External Parties	12
Manage Duplicate Use of Intersection Identifiers by External Parties	12
System Management and Recovery	14
List of Operator-Notifiable Events	14
List of Systemic Failure Events	15
Cyber Attack Must Be Addressed	16
Recovery Plan from Systemic Failure	17
Vulnerability Management for Potential Cyber Attack	18
Support Systems and Functions	20
CI System Monitoring	20
Events to be Monitored by CI System Monitoring	21

Background:

CTI4501 is undergoing an update utilizing systems engineering processes. This update aims to incorporate new insights and knowledge obtained from real-world deployments since the last version was released. The systems engineering approach ensures a comprehensive review and integration of the latest practical experiences and technological advancements into the standard.

Expansion of Security Requirements

The update process has necessitated an overhaul of security requirements, expanding the scope to encompass a broader cybersecurity perspective. This expansion reflects the evolving landscape of cybersecurity threats and the need for robust security measures across various deployment scenarios. The broadened scope ensures that the updated CTI4501 addresses current and emerging security challenges comprehensively.

Applicability to Connected Intersection Authorities

The majority of the updated security requirements are fundamental practices that connected intersection authorities should implement, regardless of whether a Roadside Unit (RSU) is deployed at an intersection. These requirements are designed to enhance overall cybersecurity posture and ensure that intersection authorities are prepared to manage cybersecurity risks effectively. For this document, however, the focus will be limited to requirements that the authorities should consider because of addition of an RSU to the intersection.

Focused Scope of RSU-Specific Requirements

The document specifically delineates requirements that either (a) apply exclusively to RSUs or (b) involve additional security controls necessitated by the installation of an RSU. By focusing on these specific scenarios, the document provides targeted guidance to ensure that RSUs are deployed and managed securely, minimizing potential vulnerabilities.

Risk-Driven Requirements and Mitigation Policies

The updated requirements are discussed in the context of the risks that prompted their inclusion, along with recommended mitigation policies. This approach ensures that each requirement is justified based on identified threats and vulnerabilities, providing a clear rationale for its implementation. The recommended policies offer practical guidance on mitigating these risks, aiding in the development of stronger security strategies.

Subset CTI4501 Security Requirements

CTI4501 introduces a framework of security requirements designed to ensure the integrity and confidentiality of connected infrastructure systems. Within this framework, certain requirements are deemed critical for Department of Transportation (DOT) implementations, even in scenarios where Vehicle-to-Everything (V2X) communications are not yet deployed. Among these, a specific subset warrants particular attention, as it pertains directly to Roadside Units (RSUs) and the integrity of their associated messaging protocols. The security requirements that DOTs should prioritize have been selectively extracted and detailed in the following table for focused implementation.

Title	Identifier	Description
Data Trustworthiness		
	SR-1.8	Integrity of Operations for Internal CI Data Entities
	SR-1.24	Events to be Monitored by Self-Monitoring
	SR-1.51	Protect V2X Radio Parameters
Intersection Identifier Trustworthiness		
	SR-12.1	Robustness of Intersection Identifier Assignment
	SR-12.2	Detect Incorrect Intersection Identifiers
	SR-12.3	Manage Incorrect Intersection Identifiers
	SR-12.4	Detect Duplicate Use of Intersection Identifiers by External Parties
	SR-12.5	Manage Duplicate Use of Intersection Identifiers by External Parties
System Management and Recovery		
	SR-13.2	List of Operator-Notifiable Events
	SR-13.3	List of Systemic Failure Events
	SR-13.4	Cyber Attack Must Be Addressed
	SR-13.5	Recovery Plan from Systemic Failure
	SR-13.12	Vulnerability Management for Potential Cyber Attack
Support Systems and Functions		
	SR-14.1	CI System Monitoring
	SR-14.2	Events to be Monitored by CI System Monitoring

Table 1: CTI4501 Selected Security Requirements

Document Structure:

This document is structured to provide a classification of the top-level requirements as defined in the CTI4501 requirements draft. Each section represents a primary requirement classification, ensuring that all relevant areas are systematically covered. Within these sections, each individual requirement is detailed as a subsection, allowing for presentation of the necessary criteria. As outlined earlier, general cybersecurity requirements in CTI4501 draft that an authority should follow and implement are not discussed here and therefore missing.

The design of this document follows a top-down approach, enabling traceability and ensuring that each requirement can be systematically linked to the associated risks and mitigations. This methodical structure is important for maintaining coherence and ensuring that the relationships between high-level requirements and their specific implications are documented.

Each requirement is uniquely identified with an identifier and a detailed description. This is followed by a table that lists the various risks associated with not implementing the requirement. These tables are critical as they not only highlight potential security vulnerabilities but also provide policy recommendations to mitigate these risks. This approach ensures that each requirement is not only understood in its own context but also in terms of its broader impact on overall security posture.

SR-1: Data Trustworthiness: Sources and Processing

SR-1.8: Integrity of Operations for Internal CI Data Entities

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

Risk ID	Risk Description	Policy Recommendations
R-001	Unauthorized access to RSU systems compromising integrity	<ul style="list-style-type: none"> - Use strong authentication methods (e.g., multi-factor authentication) - Implement role-based access control (RBAC) - Conduct regular security audits
R-002	Data integrity compromise due to malware or tampering	<ul style="list-style-type: none"> - Implement cryptographic integrity checks (e.g., digital signatures) - Use secure boot processes - Regular vulnerability assessments
R-003	Communication integrity compromise leading to false data injection	<ul style="list-style-type: none"> - Use encrypted communication channels - Maintain comprehensive logs of all communication activities, including access and modification attempts - Perform regular penetration testing to identify and mitigate potential weaknesses in the communication channels
R-004	Unauthorized firmware or software updates compromising system integrity	<ul style="list-style-type: none"> - Ensure all updates are digitally signed - Implement secure update mechanisms - Regularly verify the integrity of installed updates
R-005	Physical tampering compromising RSU integrity	<ul style="list-style-type: none"> - Use tamper-resistant enclosures - Implement tamper detection mechanisms - Conduct regular physical inspections
R-006	Insider threats leading to integrity breaches	<ul style="list-style-type: none"> - Conduct thorough background checks - Implement strict access controls - Monitor and log all access activities
R-007	System failures causing integrity issues	<ul style="list-style-type: none"> - Implement redundancy and failover mechanisms - Conduct regular system testing - Develop and test incident response plans

SR-1.24: Events to be Monitored by Self-Monitoring

For each CI data entity inside the CI, 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 SR-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
- interactions that are indicative of known cyber-attacks

SR-1.51: Protect V2X Radio Parameters

A CI Data Entity that sends C-V2X messages shall protect against the C-V2X radio parameters being modified such that the requirements in 3.3.1.2 are not conformed to.

Risk ID	Risk Description	Policy Recommendations
R-008	Modification of C-V2X radio parameters compromising compliance with 3.3.1.2	<ul style="list-style-type: none"> - Implement access controls to restrict modification of radio parameters - Monitor and log all changes to radio parameters - Regularly audit configurations to ensure compliance - Use secure firmware and software updates to protect configurations - Conduct regular training for personnel on secure configuration management - Implement anomaly detection systems to identify unauthorized changes - Ensure redundancy and backup of configuration settings to quickly restore compliant states

SR-12: Intersection Identifier Trustworthiness

SR-12.1: Robustness of Intersection Identifier Assignment

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

Risk ID	Risk Description	Policy Recommendations
R-150	Failure to document intersection identifier assignment processes, leading to potential mismanagement and inconsistencies	<ul style="list-style-type: none"> - Develop and maintain comprehensive documentation for the intersection identifier assignment process - Include detailed procedures for assigning, managing, and auditing intersection identifiers - Regularly review and update documentation to reflect any process changes - Provide training for personnel on following the documented processes
R-151	Risk of assigning the same identifier to more than one intersection, potentially causing data and traffic management issues	<ul style="list-style-type: none"> - Implement validation checks to ensure unique identifier assignment - Use a centralized database to manage and track assigned identifiers - Regularly audit the identifier assignment process to identify and correct any duplications - Develop and enforce policies to handle and resolve identifier conflicts
R-152	High reliance on manual processes for assigning intersection identifiers, leading to potential human errors	<ul style="list-style-type: none"> - Automate the identifier assignment process to minimize human errors - Implement automated validation checks to ensure unique assignments - Regularly test and validate the automated systems for accuracy and reliability - Conduct regular training for personnel on using automated tools for identifier assignment
R-153	Inadequate documentation and communication of intersection identifier assignment policies, resulting in inconsistent application across CIs	<ul style="list-style-type: none"> - Standardize the identifier assignment process across all CIs - Ensure clear communication of assignment policies to all relevant personnel - Develop comprehensive guidelines and best practices for intersection identifier assignment - Conduct regular training sessions and workshops to reinforce policy understanding
R-154	Potential impact on data integrity and traffic management due to duplicate intersection identifiers	<ul style="list-style-type: none"> - Implement monitoring systems to detect and alert on identifier duplication - Regularly verify the integrity and uniqueness of assigned identifiers - Conduct impact assessments to understand and mitigate the effects of identifier duplication - Engage with stakeholders to ensure adherence to best practices and industry standards

SR-12.2: Detect Incorrect Intersection Identifiers

A CI 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 CI uses an identifier other than the one assigned to that intersection.

Risk ID	Risk Description	Policy Recommendations
R-155	Failure to detect SPaT or MAP messages using incorrect identifiers, leading to potential traffic management issues and data integrity risks	<ul style="list-style-type: none"> - Implement real-time monitoring systems to detect incorrect intersection identifiers - Use validation checks to ensure SPaT and MAP messages use the correct identifiers - Regularly update and test detection mechanisms to maintain accuracy
R-156	Incorrect SPaT or MAP message data due to using incorrect identifiers, potentially resulting in incorrect traffic management decisions	<ul style="list-style-type: none"> - Monitor and log all SPaT and MAP message data and validation results - Implement cross-checks with intersection identifier records to ensure accuracy - Conduct regular audits and assessments of identifier consistency - Provide ongoing training for personnel on the importance of accurate identifier usage
R-157	Delay in detecting incorrect identifiers, causing lag in corrective actions and impacting traffic flow	<ul style="list-style-type: none"> - Establish real-time alert systems for immediate notification of incorrect identifiers - Optimize detection processes to minimize delay - Implement redundant monitoring systems to ensure continuous operation - Conduct regular drills and training for personnel on timely detection and response procedures
R-158	High processing load due to identifier consistency checks, potentially impacting CI performance	<ul style="list-style-type: none"> - Optimize consistency check algorithms to minimize processing overhead - Implement hardware acceleration where possible to support intensive checks - Regularly evaluate and update processing capabilities to handle expected data loads - Implement scalable solutions to maintain performance during peak traffic times
R-159	Inadequate documentation and communication of identifier consistency check policies, resulting in inconsistent application across CIs	<ul style="list-style-type: none"> - Develop comprehensive documentation for identifier consistency check policies and procedures - Standardize consistency check practices across all CIs - Ensure clear communication of policies to all relevant personnel - Conduct regular training sessions and workshops to reinforce policy understanding

SR-12.3: Manage Incorrect Intersection Identifiers

If a SPaT or MAP message that is intended to refer to a particular intersection within the CI 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 a central monitoring system 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, optionally, inform receivers of that information that the information is not available. Additional mitigations may also be implemented.

Risk ID	Risk Description	Policy Recommendations
R-160	Failure to manage incorrect intersection identifiers in SPaT or MAP messages, leading to potential traffic management issues and data integrity risks	<ul style="list-style-type: none"> - Develop and document a comprehensive policy for managing incorrect identifiers - Ensure the policy includes automatic recovery, central system notification, direct operator notification, local logging, and stopping message transmission if needed - Regularly review and update the policy to address new scenarios and technologies - Provide training for personnel on the policy and its implementation
R-161	Incorrect SPaT or MAP message data due to using incorrect identifiers not being addressed promptly, causing confusion and potential safety risks	<ul style="list-style-type: none"> - Implement automated systems for detecting and attempting to recover from incorrect identifiers - Ensure the CI can validate successful recovery - Establish real-time notification systems to inform a central monitoring system or operators - Implement logging mechanisms to record failures and actions taken - Develop procedures for stopping V2X message transmission if inconsistencies cannot be resolved
R-162	Delays in operator or central system response to detected incorrect identifiers, impacting traffic flow and safety	<ul style="list-style-type: none"> - Optimize notification processes to minimize delay in informing central systems or operators - Implement redundant communication channels to ensure notifications are received - Conduct regular training and drills for operators on responding to incorrect identifier notifications - Establish clear escalation protocols for handling unresolved identifier issues
R-163	High reliance on manual intervention for managing incorrect identifiers, leading to potential human errors	<ul style="list-style-type: none"> - Automate as many inconsistency management actions as possible to reduce reliance on manual intervention - Implement validation checks to ensure automatic actions are successful - Provide ongoing training for personnel on using automated tools and managing exceptions - Regularly test and update automated systems to maintain accuracy and reliability
R-164	Inadequate documentation and communication of identifier management policies, resulting in inconsistent application across CIs	<ul style="list-style-type: none"> - Develop comprehensive documentation for identifier management policies and procedures - Standardize identifier management practices across all CIs - Ensure clear communication of policies to all relevant personnel - Conduct regular training sessions and workshops to reinforce policy understanding

SR-12.4: Detect Duplicate Use of Intersection Identifiers by External Parties

A CI 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 “ego” CI even if it is not currently in use).

Risk ID	Risk Description	Policy Recommendations
R-165	Failure to detect if an external intersection uses an identifier assigned to the CI, leading to potential data integrity and traffic management issues	<ul style="list-style-type: none"> - Implement real-time monitoring systems to detect incorrect identifier use by external intersections - Use validation checks to ensure identifiers are correctly assigned and used - Regularly update and test detection mechanisms to maintain accuracy
R-166	Incorrect identifier use by an external intersection causing data and traffic management conflicts, potentially impacting the CI's operations	<ul style="list-style-type: none"> - Monitor and log all identifier use and validation results - Implement cross-checks with identifier records to ensure accuracy - Conduct regular audits and assessments of identifier usage - Provide ongoing training for personnel on the importance of accurate identifier usage
R-167	Delay in detecting incorrect identifier use by external intersections, causing lag in corrective actions and impacting traffic flow	<ul style="list-style-type: none"> - Establish real-time alert systems for immediate notification of incorrect identifier use - Optimize detection processes to minimize delay - Implement redundant monitoring systems to ensure continuous operation - Conduct regular drills and training for personnel on timely detection and response procedures
R-168	High processing load due to identifier consistency checks, potentially impacting CI performance	<ul style="list-style-type: none"> - Optimize consistency check algorithms to minimize processing overhead - Implement hardware acceleration where possible to support intensive checks - Regularly evaluate and update processing capabilities to handle expected data loads - Implement scalable solutions to maintain performance during peak traffic times
R-169	Inadequate documentation and communication of identifier consistency check policies, resulting in inconsistent application across CIs	<ul style="list-style-type: none"> - Develop comprehensive documentation for identifier consistency check policies and procedures - Standardize consistency check practices across all CIs - Ensure clear communication of policies to all relevant personnel - Conduct regular training sessions and workshops to reinforce policy understanding

SR-12.5: Manage Duplicate Use of Intersection Identifiers by External Parties

A CI 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 “ego” CI even if it is not currently in use).

Risk ID	Risk Description	Policy Recommendations
R-170	Failure to manage incorrect identifier use by external intersections, leading to potential data integrity and traffic management issues	<ul style="list-style-type: none"> - Develop and document a comprehensive policy for managing incorrect identifier use - Ensure the policy includes automatic recovery, central system notification, direct operator notification, local logging, and stopping message transmission if needed - Regularly review and update the policy to address new scenarios and technologies - Provide training for personnel on the policy and its implementation
R-171	Incorrect identifier use by an external intersection causing data and traffic management conflicts, potentially impacting the CI's operations	<ul style="list-style-type: none"> - Implement automated systems for detecting and attempting to recover from incorrect identifier use - Ensure the CI can validate successful recovery - Establish real-time notification systems to inform a central monitoring system or operators - Implement logging mechanisms to record failures and actions taken - Develop procedures for stopping V2X message transmission if inconsistencies cannot be resolved
R-172	Delays in operator or central system response to detected incorrect identifier use, impacting traffic flow and safety	<ul style="list-style-type: none"> - Optimize notification processes to minimize delay in informing central systems or operators - Implement redundant communication channels to ensure notifications are received - Conduct regular training and drills for operators on responding to incorrect identifier notifications - Establish clear escalation protocols for handling unresolved identifier issues
R-173	High reliance on manual intervention for managing incorrect identifiers, leading to potential human errors	<ul style="list-style-type: none"> - Automate as many inconsistency management actions as possible to reduce reliance on manual intervention - Implement validation checks to ensure automatic actions are successful - Provide ongoing training for personnel on using automated tools and managing exceptions - Regularly test and update automated systems to maintain accuracy and reliability
R-174	Inadequate documentation and communication of identifier management policies, resulting in inconsistent application across CIs	<ul style="list-style-type: none"> - Develop comprehensive documentation for identifier management policies and procedures - Standardize identifier management practices across all CIs - Ensure clear communication of policies to all relevant personnel - Conduct regular training sessions and workshops to reinforce policy understanding

SR-13: System Management and Recovery

SR-13.2: List of Operator-Notifiable Events

The CI shall identify system monitoring events (or types of events) for the system monitoring function shall notify a human operator.

Risk ID	Risk Description	Policy Recommendations
R-175	Failure to identify system monitoring events requiring human operator notification, leading to potential oversight of critical issues	<ul style="list-style-type: none">- Develop and document comprehensive criteria for identifying system monitoring events that require human operator notification- Regularly review and update the criteria to address new types of events and technologies- Provide training for personnel on identifying and responding to these events- Implement automated systems to detect and flag these events for operator notification
R-176	Delayed response to critical system monitoring events due to lack of timely notification to human operators, potentially impacting system performance and safety	<ul style="list-style-type: none">- Establish real-time monitoring and alert systems to notify operators immediately of critical events- Implement redundant communication channels to ensure notifications are received promptly- Conduct regular drills and training for operators on responding to notifications- Develop clear escalation protocols for handling critical events
R-177	High reliance on manual processes for monitoring and identifying critical events, leading to potential human errors	<ul style="list-style-type: none">- Automate the identification and notification processes to minimize human errors- Implement validation checks to ensure critical events are correctly identified and flagged- Regularly test and validate the automated systems for accuracy and reliability- Conduct regular training for personnel on using automated monitoring and notification tools
R-178	Inadequate documentation and communication of monitoring and notification policies, resulting in inconsistent application across RSUs	<ul style="list-style-type: none">- Develop comprehensive documentation for monitoring and notification policies and procedures- Standardize monitoring and notification practices across all RSUs- Ensure clear communication of policies to all relevant personnel- Conduct regular training sessions and workshops to reinforce policy understanding

Risk ID	Risk Description	Policy Recommendations
R-179	Potential impact on system integrity and reliability due to missed or delayed notifications of critical events	<ul style="list-style-type: none"> - Regularly verify the effectiveness of monitoring and notification systems - Implement monitoring systems to detect and alert on any missed or delayed notifications - Conduct regular assessments to ensure the monitoring and notification processes meet required standards - Engage with stakeholders to ensure alignment with best practices and industry standards

SR-13.3: List of Systemic Failure Events

The CI shall have a list of systemic failure events for which a recovery plan shall be specified (for example, due to cyber attacks, power outages, physical events, etc).

Risk ID	Risk Description	Policy Recommendations
R-180	Failure to have a comprehensive list of systemic failure events, leading to potential unpreparedness for critical incidents	<ul style="list-style-type: none"> - Develop and document a comprehensive list of systemic failure events, including cyber attacks, power outages, and physical events - Regularly review and update the list to include new types of events and threats - Conduct risk assessments to prioritize events based on their potential impact - Provide training for personnel on identifying and reporting systemic failure events
R-181	Lack of specified recovery plans for systemic failure events, potentially causing prolonged system downtime and safety risks	<ul style="list-style-type: none"> - Develop detailed recovery plans for each identified systemic failure event - Ensure recovery plans include steps for immediate response, mitigation, and system restoration - Regularly test and update recovery plans to ensure their effectiveness - Conduct regular training and drills for personnel on executing recovery plans
R-182	Delayed response to systemic failure events due to lack of preparedness, impacting system performance and safety	<ul style="list-style-type: none"> - Establish real-time monitoring and alert systems to detect and respond to systemic failure events promptly - Implement automated systems to initiate recovery actions where possible - Develop clear escalation protocols for handling systemic failure events - Provide training for personnel on rapid response and recovery techniques

Risk ID	Risk Description	Policy Recommendations
R-183	High reliance on manual processes for managing systemic failure events, leading to potential human errors	<ul style="list-style-type: none"> - Automate the detection and initial response processes for systemic failure events to minimize human errors - Implement validation checks to ensure recovery plans are correctly followed - Regularly test and validate the automated systems for accuracy and reliability - Conduct regular training for personnel on using automated tools for managing systemic failure events
R-184	Inadequate documentation and communication of recovery plans, resulting in inconsistent application across CIs	<ul style="list-style-type: none"> - Develop comprehensive documentation for recovery plans and procedures for systemic failure events - Standardize recovery plan practices across all CIs - Ensure clear communication of recovery plans to all relevant personnel - Conduct regular training sessions and workshops to reinforce understanding of recovery plans

SR-13.4: Cyber Attack Must Be Addressed

The list specified in SR-13.2 shall include cyber attacks as a systemic failure event to be considered.

Risk ID	Risk Description	Policy Recommendations
R-185	Failure to include cyber attacks in the list of systemic failure events, leading to unpreparedness for such incidents	<ul style="list-style-type: none"> - Ensure cyber attacks are explicitly listed as a systemic failure event in the CI's documentation - Regularly review and update the list to include emerging cyber threats - Conduct risk assessments to prioritize cyber attacks based on their potential impact - Provide training for personnel on identifying and responding to cyber attacks
R-186	Lack of specified recovery plans for cyber attacks, potentially causing prolonged system downtime and security risks	<ul style="list-style-type: none"> - Develop detailed recovery plans specifically for cyber attack scenarios - Ensure recovery plans include steps for immediate response, mitigation, and system restoration - Regularly test and update recovery plans to ensure their effectiveness against cyber threats - Conduct regular training and drills for personnel on executing cyber attack recovery plans
R-187	Delayed response to cyber attacks due to lack of preparedness, impacting system performance and security	<ul style="list-style-type: none"> - Establish real-time monitoring and alert systems to detect and respond to cyber attacks promptly - Implement automated systems to initiate recovery actions where possible - Develop clear escalation protocols for handling cyber attacks - Provide training for personnel on rapid response and recovery techniques for cyber incidents

Risk ID	Risk Description	Policy Recommendations
R-188	High reliance on manual processes for managing cyber attacks, leading to potential human errors	<ul style="list-style-type: none"> - Automate the detection and initial response processes for cyber attacks to minimize human errors - Implement validation checks to ensure recovery plans are correctly followed during a cyber attack - Regularly test and validate the automated systems for accuracy and reliability - Conduct regular training for personnel on using automated tools for managing cyber attacks
R-189	Inadequate documentation and communication of recovery plans for cyber attacks, resulting in inconsistent application across CIs	<ul style="list-style-type: none"> - Develop comprehensive documentation for cyber attack recovery plans and procedures - Standardize cyber attack recovery practices across all CIs - Ensure clear communication of recovery plans to all relevant personnel - Conduct regular training sessions and workshops to reinforce understanding of cyber attack recovery plans

SR-13.5: Recovery Plan from Systemic Failure

For each systemic failure event in the list, the CI shall have a plan to recover from that event and to validate such recovery for the system.

Risk ID	Risk Description	Policy Recommendations
R-190	Lack of a recovery plan for systemic RSU failure events, leading to potential unpreparedness and prolonged system downtime	<ul style="list-style-type: none"> - Develop detailed recovery plans for each identified systemic RSU failure event - Ensure recovery plans include steps for immediate response, mitigation, and system restoration - Regularly test and update recovery plans to ensure their effectiveness - Conduct regular training and drills for personnel on executing recovery plans
R-191	Failure to validate recovery from systemic RSU failure events, potentially causing incomplete or ineffective recovery	<ul style="list-style-type: none"> - Implement validation processes to ensure recovery steps are correctly executed and successful - Use automated tools and systems to assist in the validation of recovery processes - Regularly review and update validation procedures to address new failure scenarios - Provide training for personnel on validating recovery processes
R-192	Delayed response to systemic RSU failure events due to lack of preparedness, impacting system performance and safety	<ul style="list-style-type: none"> - Establish real-time monitoring and alert systems to detect and respond to systemic RSU failure events promptly - Implement automated systems to initiate recovery actions where possible - Develop clear escalation protocols for handling systemic RSU failure events - Provide training for personnel on rapid response and recovery techniques

Risk ID	Risk Description	Policy Recommendations
R-193	High reliance on manual processes for managing systemic RSU failure events, leading to potential human errors	<ul style="list-style-type: none"> - Automate the detection and initial response processes for systemic RSU failure events to minimize human errors - Implement validation checks to ensure recovery plans are correctly followed - Regularly test and validate the automated systems for accuracy and reliability - Conduct regular training for personnel on using automated tools for managing systemic RSU failure events
R-194	Inadequate documentation and communication of recovery plans, resulting in inconsistent application across CIs	<ul style="list-style-type: none"> - Develop comprehensive documentation for recovery plans and procedures for systemic RSU failure events - Standardize recovery plan practices across all CIs - Ensure clear communication of recovery plans to all relevant personnel - Conduct regular training sessions and workshops to reinforce understanding of recovery plans

SR-13.12: Vulnerability Management for Potential Cyber Attack

A CI 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.

Risk ID	Risk Description	Policy Recommendations
R-195	Lack of a process to be informed of potential vulnerabilities in CI data entities, leading to unaddressed security risks	<ul style="list-style-type: none"> - Establish a formal process for vulnerability information gathering from multiple sources, including threat intelligence feeds, security advisories, and vendor notifications - Regularly review and update the process to include new sources and methods for identifying potential vulnerabilities - Provide training for personnel on identifying and reporting potential vulnerabilities
R-196	Failure to determine whether potential vulnerabilities lead to risks, resulting in unmitigated threats to CI data entities	<ul style="list-style-type: none"> - Implement a risk assessment framework to evaluate the potential impact and likelihood of identified vulnerabilities - Use automated tools and systems to assist in the risk assessment process - Regularly review and update the risk assessment framework to address new vulnerabilities and threats - Provide training for personnel on conducting thorough risk assessments
R-197	Delayed response to identified risks from potential vulnerabilities, impacting system performance and security	<ul style="list-style-type: none"> - Establish a real-time monitoring and alert system to detect and respond to identified risks promptly - Implement automated systems to initiate risk mitigation actions where possible - Develop clear escalation protocols for handling significant risks - Provide training for personnel on rapid response and risk mitigation techniques

Risk ID	Risk Description	Policy Recommendations
R-198	High reliance on manual processes for managing potential vulnerabilities, leading to potential human errors	<ul style="list-style-type: none">- Automate the identification, assessment, and mitigation processes for potential vulnerabilities to minimize human errors- Implement validation checks to ensure risk assessments and mitigation actions are correctly executed- Regularly test and validate the automated systems for accuracy and reliability- Conduct regular training for personnel on using automated tools for managing potential vulnerabilities
R-199	Inadequate documentation and communication of the vulnerability management process, resulting in inconsistent application across CIs	<ul style="list-style-type: none">- Develop comprehensive documentation for the vulnerability management process, including identification, assessment, and mitigation procedures- Standardize vulnerability management practices across all CIs- Ensure clear communication of the process to all relevant personnel- Conduct regular training sessions and workshops to reinforce understanding of the vulnerability management process

SR-14: Support Systems and Functions

SR-14.1: CI System Monitoring

The CI shall support a system monitoring function. This system monitoring function shall record 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 SR-14.2.

Risk ID	Risk Description	Policy Recommendations
R-200	Failure to implement a system monitoring function, leading to unmonitored system states and undetected issues	<ul style="list-style-type: none"> - Establish and document a comprehensive system monitoring function that records the state of the system - Regularly review and update the monitoring function to include new hardware, software, and security-relevant events - Provide training for personnel on using the system monitoring function
R-201	Inadequate recording of hardware and software configurations, potentially causing incomplete or inaccurate system state records	<ul style="list-style-type: none"> - Implement automated tools to record hardware and software configurations of all CI data entities - Use standardized formats and protocols for recording configurations - Conduct regular audits and reviews of recorded configurations to ensure accuracy - Provide training for personnel on recording and updating hardware and software configurations
R-202	Failure to record relevant version information, leading to potential inconsistencies and difficulties in system management	<ul style="list-style-type: none"> - Develop a version control system to record relevant version information for all CI data entities - Regularly update version information records to reflect changes and updates - Conduct regular audits and reviews of version information to ensure completeness - Provide training for personnel on recording and managing version information
R-203	Incomplete recording of security-relevant events, potentially causing undetected security incidents and vulnerabilities	<ul style="list-style-type: none"> - Implement a security event logging system to record all specified security-relevant events - Regularly review and update the list of security-relevant events to be recorded - Conduct regular audits and reviews of security event logs to ensure completeness and accuracy - Provide training for personnel on identifying and recording security-relevant events
R-204	High reliance on manual processes for system monitoring, leading to potential human errors	<ul style="list-style-type: none"> - Automate the system monitoring function to minimize human errors - Implement validation checks to ensure monitoring data is accurately recorded - Regularly test and validate the automated monitoring systems for accuracy and reliability - Conduct regular training for personnel on using automated monitoring tools

Risk ID	Risk Description	Policy Recommendations
R-205	Delayed detection and response to system state changes or security incidents due to inadequate monitoring	<ul style="list-style-type: none"> - Establish real-time monitoring and alert systems to detect and respond to system state changes and security incidents promptly - Implement automated systems to initiate response actions where possible - Develop clear escalation protocols for handling detected incidents - Provide training for personnel on rapid response and incident management techniques
R-206	Inadequate documentation and communication of the system monitoring process, resulting in inconsistent application across CIs	<ul style="list-style-type: none"> - Develop comprehensive documentation for the system monitoring process, including recording, auditing, and responding to system states and events - Standardize monitoring practices across all CIs - Ensure clear communication of the monitoring process to all relevant personnel - Conduct regular training sessions and workshops to reinforce understanding of the monitoring process
R-207	Potential impact on system performance and security due to incomplete or inaccurate monitoring data	<ul style="list-style-type: none"> - Regularly verify the integrity and reliability of monitoring data - Implement monitoring systems to detect and alert on discrepancies or missing data - Conduct regular assessments to ensure the monitoring function meets required standards - Engage with stakeholders to ensure alignment with best practices and industry standards

SR-14.2: Events to be Monitored by CI System Monitoring

The events covered by the CI system monitoring function shall include the following: (Optional)

- 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 SR-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 cyber-attacks

Recommended Security Policies

Automation of Processes

Automating processes is an effective security policy because it reduces the risk of human error, which is a significant factor in security breaches. Automated systems can consistently apply security protocols, manage configurations, and monitor for threats without the variability introduced by manual interventions. This consistency enhances the reliability of security measures, ensuring that policies are enforced uniformly across an organization. Moreover, automation can swiftly respond to security incidents, minimizing potential damage and maintaining compliance with security standards.

Processes that should be covered include:

- Automate configuration management processes to minimize human errors.
- Automate MAP message generation processes to minimize human errors.
- Automate MAP message update processes to minimize human errors.
- Automate the configuration and monitoring processes for RSU radio coverage to minimize human errors.
- Automate the configuration and monitoring processes for RSU radio transmit power to minimize human errors.
- Automate the detection and initial response processes for cyber attacks to minimize human errors.
- Automate the detection and initial response processes for systemic failure events to minimize human errors.
- Automate the detection and monitoring processes for RSU radio coverage to minimize human errors.
- Automate the detection and monitoring processes for RSU radio transmit power to minimize human errors.
- Automate the identification and notification processes to minimize human errors.
- Automate the identification, assessment, and mitigation processes for potential vulnerabilities to minimize human errors.
- Automate the system monitoring function to minimize human errors.

Audits and Assessments

Audits and assessments are critical components of a robust security policy because they provide a systematic method for evaluating the effectiveness of security controls. Regular audits ensure that security measures are being properly implemented and maintained, helping to identify any weaknesses or gaps that could be exploited by attackers. Assessments, on the other hand, allow organizations to continuously improve their security posture by analyzing the current threat landscape and adapting their strategies accordingly. Together, they ensure that security practices remain aligned with organizational goals and evolving risks.

Some examples of these include:

- Conduct regular audits and assessments of consistency checks.
- Conduct regular audits and assessments of external data sources and processors.
- Conduct regular audits and assessments of identifier consistency.
- Conduct regular audits and assessments of identifier usage.
- Conduct regular audits and assessments of MAP message consistency.
- Conduct regular audits and assessments of the timing consistency and freshness check processes.

-
- Conduct regular audits and reviews of AGP initiation processes.
 - Conduct regular audits and reviews of MAP-impacting CI data entities.
 - Conduct regular audits and reviews of RDZ configurations.
 - Conduct regular audits and reviews of recorded configurations to ensure accuracy.
 - Conduct regular audits and reviews of RSU configurations.
 - Conduct regular audits and reviews of RTCM-impacting CI data entities.
 - Conduct regular audits and reviews of security event logs to ensure completeness and accuracy.
 - Conduct regular audits and reviews of SPaT-impacting CI data entities.
 - Conduct regular audits and reviews of version information to ensure completeness.

Training and Drills

Training and drills are essential for strengthening an organization's security posture because they prepare personnel to respond effectively to real-world threats. Regular training ensures that staff are knowledgeable about security protocols and best practices, reducing the likelihood of errors during critical situations. Drills simulate various attack scenarios, allowing teams to practice and refine their response strategies in a controlled environment. This proactive approach enhances readiness, ensuring that everyone is equipped to handle incidents swiftly and efficiently, minimizing potential damage and disruptions.

Examples include:

- Conduct regular coordination and training sessions for RSU operators.
- Conduct regular drills and training for operators on responding to notifications.
- Conduct regular drills and training for personnel on timely reporting procedures.
- Conduct regular training and drills for personnel on executing cyber attack recovery plans.
- Conduct regular training sessions and workshops to reinforce understanding of cyber attack recovery plans.
- Conduct regular training sessions and workshops to reinforce understanding of the monitoring process.
- Conduct regular training sessions and workshops to reinforce understanding of the vulnerability management process.

Documented Security Policies and Procedures

Documented security policies and procedures are vital because they provide a clear framework for implementing and maintaining security measures across an organization. These documents outline specific roles, responsibilities, and protocols, ensuring consistency and compliance with regulatory requirements. By clearly defining expectations and processes, documented policies reduce ambiguity, helping to prevent security incidents caused by miscommunication or lack of understanding. Additionally, they serve as a reference point during audits and assessments, demonstrating the organization's commitment to security best practices.

Key ones to consider:

- Develop and enforce policies for timely response to detected changes.
- Develop and enforce policies for timely response to detected configuration issues.

-
- Develop and enforce policies to handle and resolve identifier conflicts.
 - Develop and implement policies for the application of trust levels in message validation.
 - Develop and implement validation checks to confirm changes in intersection geometry or use are properly reflected in MAP messages.
 - Develop and implement validation checks to confirm changes in intersection geometry or use before sending MAP updates.
 - Develop and maintain comprehensive documentation for the intersection identifier assignment process.
 - Develop comprehensive documentation for AGP initiation policies and procedures.
 - Develop comprehensive documentation for BSM filtering policies and procedures.
 - Develop comprehensive documentation for consistency assurance policies and procedures.

Monitoring and Logging

Monitoring and logging are critical components of an effective security strategy because they provide continuous oversight of an organization's systems and data. Monitoring allows for real-time detection of suspicious activities, enabling swift responses to potential threats. Logging, on the other hand, ensures that all actions within the system are recorded and can be reviewed for forensic analysis, audits, and compliance verification. Together, they create a robust mechanism for identifying, analyzing, and responding to security incidents, ultimately helping to prevent breaches and maintain system integrity.

The following should be taken into consideration for V2X enabled intersections:

- Monitor and log all access activities.
- Monitor and log all AGP initiation events.
- Monitor and log all changes to MAP-impacting CI data entities.
- Monitor and log all changes to radio parameters.
- Monitor and log all changes to RSU radio coverage settings.
- Monitor and log all changes to RSU radio transmit power settings.
- Monitor and log all changes to RTCM-impacting CI data entities.
- Monitor and log all changes to signal timing data configurations.
- Monitor and log all changes to SPaT-impacting CI data entities.
- Monitor and log all changes to the list.

Validation and Verification

Validation and verification of V2X (Vehicle-to-Everything) data are crucial for ensuring the accuracy, integrity, and reliability of communications between vehicles and infrastructure. Validation ensures that the data being transmitted conforms to expected formats and protocols, while verification confirms that the data is both accurate and authentic. These processes help prevent malicious activities, such as spoofing or data tampering, and ensure that the V2X system functions correctly, supporting safe and efficient transportation operations. Regular validation and verification enhance trust in the system and reduce the risk of accidents caused by incorrect or malicious data.

Key ones include:

- Implement validation checks for data received from external sources.
- Implement validation checks for reported data.
- Implement validation checks to compare generated SPaT messages with RSU data and physical signals.
- Implement validation checks to compare new messages with recently received ones.
- Implement validation checks to ensure BSM filtering is enabled and correctly configured.
- Implement validation checks to ensure critical events are correctly identified and flagged.
- Implement validation checks to ensure MAP-impacting CI data entities remain conformant.
- Implement validation checks to ensure MAP messages are only updated when necessary.
- Implement validation checks to ensure MAP messages are updated accurately when changes occur.
- Implement validation checks to ensure monitoring data is accurately recorded.

Risk Management and Recovery

Risk management and recovery are essential for maintaining organizational resilience against security threats. Risk management involves identifying, assessing, and prioritizing risks to minimize potential damage. It enables organizations to implement controls that mitigate threats before they materialize. Recovery planning, on the other hand, ensures that an organization can quickly return to normal operations after a security incident. This includes having a well-documented incident response plan and conducting regular drills to prepare for various scenarios. Together, these practices help minimize disruption and protect critical assets during and after an incident.

Organisations are strongly recommended to:

- Conduct risk assessments to prioritize cyber attacks based on their potential impact.
- Conduct risk assessments to prioritize events based on their potential impact.
- Develop and document comprehensive criteria for identifying system monitoring events that require human operator notification.
- Develop and document a comprehensive policy for action upon detecting inconsistencies.
- Develop and document a comprehensive policy for managing inconsistencies.
- Develop and document a comprehensive policy for managing incorrect identifiers.
- Develop and document a comprehensive policy for managing incorrect identifier use.
- Develop clear escalation protocols for handling critical events.
- Develop clear escalation protocols for handling cyber attacks.
- Develop clear escalation protocols for handling detected incidents.

Cryptography and Secure Communication

Cryptography and secure communications are fundamental to protecting data integrity, confidentiality, and authenticity in digital interactions. Cryptography uses mathematical algorithms to encrypt data, making it unintelligible to unauthorized users, while secure communication protocols ensure that data is transmitted safely between parties. These practices prevent eavesdropping, data tampering, and unauthorized access, ensuring that sensitive information remains protected during transmission. By implementing strong cryptographic measures and secure communication channels, organizations can safeguard against cyber threats and maintain the trustworthiness of their digital infrastructure.

-
- Ensure all updates are digitally signed.
 - Ensure all V2X messages are authenticated before use.
 - Use cryptographic methods to ensure data integrity and authenticity.
 - Use cryptographic methods to ensure the integrity of radio configuration data.
 - Use cryptographic methods to ensure the integrity of transmit power configuration data.
 - Utilize cryptographic methods to verify the integrity and authenticity of received messages.
 - Use encrypted communication channels.
 - Use secure boot processes.
 - Use tamper-resistant enclosures.

Glossary

Authentication

The process of verifying the identity of a user or system.

Authorization

The process of granting or denying access to resources based on the identity that was authenticated.

C-V2X

Cellular Vehicle-to-Everything, a V2X communication technology that uses cellular networks for communication between vehicles and infrastructure.

Connected Intersection

An intersection where traffic signals and other infrastructure communicate with vehicles to improve traffic flow and safety.

DSRC

Dedicated Short Range Communications, a communication protocol specifically designed for automotive use to enable V2X communication.

Encryption

The process of converting information into a secure format that can only be read by authorized parties.

Firewall

A network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

Intrusion Detection System (IDS)

A device or software application that monitors a network or systems for malicious activity or policy violations.

RSU

Roadside Unit, a device installed along the road that enables V2X communication between vehicles and infrastructure.

SPaT

Signal Phase and Timing, a communication protocol that allows traffic signals to convey their status and timing information to vehicles.

V2I

Vehicle-to-Infrastructure communication, a type of V2X communication where vehicles communicate with road infrastructure such as traffic signals and road signs.

V2N

Vehicle-to-Network communication, a type of V2X communication where vehicles communicate with cellular networks and other network services.

V2P

Vehicle-to-Pedestrian communication, a type of V2X communication where vehicles communicate with pedestrians.

V2V

Vehicle-to-Vehicle communication, a type of V2X communication where vehicles exchange information directly.

V2X

Vehicle-to-Everything, a communication system that allows vehicles to communicate with each other and with infrastructure.