CSA GROUP™

STANDARDS RESEARCH

Physical and Digital Infrastructure for Connected and Automated Vehicles (CAV)

Code Framework

October 2021

Authors

Shawn Kimmel, Ph.D., QS-2 Director of Engineering

Adam Duran, QS-2 Senior Engineer

Jeremiah Robertson, QS-2 Senior Engineer

Michaela Vanderveen, Ph.D., QS-2 Lead Engineer

Barbara Wendling, QS-2 Senior Engineer

Project Advisory Panel

Jonathan Parent, Transport Canada

Edward Straub, SAE International

Paul Carlson, Road Infrastructure Inc.

Brent Harman, CSA Group

Mahmood Nesheli, CSA Group (Project Manager)

Nikki Kidd, CSA Group

Acknowledgements

The authors would like to acknowledge the participation of our industry stakeholders who volunteered their time to share their expertise and insights on the current state of connected and automated vehicle (CAV) technology standards.

This report is supported by Canadian Standards Association (operating as CSA Group) and is complementary to other initiatives undertaken by Canadian Standards Association with funding received from Transport Canada's Program to Advance Connectivity and Automation in the Transportation System (ACATS).

Disclaimer

This work has been produced by QS-2 and is owned by Canadian Standards Association. It is designed to provide general information in regards to the subject matter covered. The views expressed in this publication are those of the authors. QS-2 and Canadian Standards Association are not responsible for any loss or damage which might occur as a result of your reliance or use of the content in this publication.

Table of Contents

Executive Summary

The CSA Group report titled "Connected and Automated Vehicle Technologies – Insights for Codes and Standards in Canada" provided recommendations and highlighted the need for a code that provides requirements and specifications for digital and physical infrastructure to be safely installed and securely operated in supporting connected and automated vehicle (CAV) technology deployment [1]. To help meet that need, this report provides a framework for developing a code relevant for CAV implementation within North America as it relates to three topic areas: 1) physical infrastructure, 2) digital infrastructure, and 3) cybersecurity and data security/privacy. The development of the framework was informed by an investigation into relevant standards, technical research, and other existing literature sources. In addition, the findings in this report are also informed based on interviews with several experts within the physical and digital infrastructure fields that provided input on emerging standards and validated findings from the literature review. Categories for CAV requirements and specifications, as well as many relevant standards within these categories, are identified providing a framework that serves as a tractable starting point for a CAV code.

Results from the literature review and interviews identified several key findings for a North American framework for digital and physical infrastructure:

- Physical Infrastructure
  - Consistent and well-maintained physical infrastructure can improve reliability of CAVs, especially by improving performance of onboard sensors.
  - Design standards may facilitate CAV deployments, especially for markings, signage, and signals.
  - Design standards run the risk of being so tailored to specific vehicle sensor technologies that they may become obsolete due to rapidly advancing technology.
- Digital Infrastructure
  - Interoperability of instrumented infrastructure and vehicles is critical to capturing benefits, which motivates the need for standardized protocols, message sets, and dialogues.
  - Cooperative driving automation features are enabled by standardized use case definitions and performance requirements that are agnostic of communications technology.
  - High-definition maps are enabled by timely and accurate data about changes to road infrastructure (e.g., work zones and utility work).
- Cybersecurity and Data/Security Privacy
  - There are numerous communications pathways (e.g., 4G/5G, DSRC/C-V2X, NFC, Satellite, Wi-Fi, Bluetooth) by which CAVs exchange data with infrastructure, and each comes with privacy and security challenges.
  - While cybersecurity can look different for each organization, there are well-established security frameworks and engineering practices that can improve a system-wide security posture. In particular, there is a need for guidance tailored to help public sector agencies assess and mitigate cybersecurity risks with limited resources.
  - Privacy is governed by legal and regulatory frameworks at international, national, and local levels.

"The CAV code will be valuable to manufacturers, infrastructure owner/operators, and regulators who will be able to reference the document to further promote interoperability across North America."

1. Introduction

In June 2020, a report titled "Connected and Automated Vehicle Technologies – Insights for Codes and Standards in Canada" [1] was published by CSA Group, providing recommendations and outlining areas where Canada can provide leadership in connected and automated vehicle (CAV) deployment. One key recommendation drawn from the report is the need for the development of a CAV code for physical infrastructure (e.g., signals, signage, lane markings, and roads) and digital infrastructure (e.g., roadside sensors, communication protocols, Global Positioning System [GPS], and high-definition [HD] mapping). Infrastructure is critical to provide interoperability among different automated driving systems (ADSs) designed and built by various manufacturers, however installation requirements have not yet been established for Canada or the United States. Although there have been standardization efforts in Canada and internationally to address aspects of infrastructure-based safety, there is a lack of understanding of which requirements are needed for CAV deployment in the near-term.

A CAV code has been identified as an effective approach to establishing infrastructure installation requirements by adding the appropriate context for the relevant standards and their application to promote a safe and interoperable CAV infrastructure. As deployments become more widespread in various jurisdictions, CAV stakeholders will benefit from a consistent set of requirements to promote public safety and industry growth. It is critical to provide infrastructure installation requirements to the relevant authorities having jurisdiction while complementing Transport Canada's Safety Framework.

A CAV code will provide the requirements for CAV infrastructure installation and operation by leveraging applicable standards. The CAV code will be valuable to manufacturers, infrastructure owner/operators, and regulators who will be able to reference the document to further promote interoperability across North America.

2. Project Background

2.1 Canadian CAV Deployment Context

Infrastructure is a significant enabler for CAV technology as exemplified by the various research projects and standards development efforts occurring at national levels across North America. For example, Transport Canada's Program to Advance Connectivity and Automation in the Transportation System (ACATS) is assisting infrastructure owners and operators in Canada prepare for the wider use of CAVs on public roads [2]. Launched in 2017, this program provides provinces and territories with research funding, technology evaluations, infrastructure code development and guidance, and capacity-building and knowledge-sharing activities through development and demonstration projects. In this same year, Ottawa became the first Canadian city to test an on-street CAV that could communicate with live city infrastructure. The project involved equipping the test area infrastructure with technology to communicate with CAVs via dedicated short-range communication transmitters at traffic signals, repainting street lines, and installing controllable LED streetlights. This initiative used technology to connect 12 traffic signals with test vehicles along a six-kilometre stretch of road. The technology also notifies drivers about upcoming traffic signal changes and helps drivers determine optimum speeds to reduce fuel consumption and avoid hard braking.

As an example of the increasing need for a unified CAV code, in 2018 the cities of Vancouver and Surrey in British Columbia were selected as finalists for Infrastructure Canada's Smart City challenge to feature a collision-free, multimodal transportation corridor that linked the two cities [3]. The 3.4-kilometre corridor would have connected to several key services, including the Surrey Memorial Hospital and a major transit hub, as well as extending to Granville island and Science World near Vancouver. This initiative would include automated shuttles along the corridors, sensors in traffic signals, special lighting for road signs and markings, and other roadway infrastructure to generate real-time traffic signal data and provide signal adjustments and communications with automated shuttles. Even though the project was ultimately not selected, it signals the readiness of Canada to develop and deploy automated and smart technology enabled transportation systems and the need for a common CAV code to facilitate deployments across provinces and territories.

When considering future deployment, one needs to be cognizant of the unique features of Canadian CAV operations. There are a number of geographic, weather, and regulatory considerations that differentiate the Canadian operating environment from that of the rest of North America. For example, significant snow build-up during winter months poses a unique challenge to CAV sensor technology and routing. The Manual on Uniform Traffic Control Devices for Canada (MUTCDC) [7] is the reigning standard in Canada specifying both digital and physical infrastructure design guidance, although its guidance remains voluntary at the provincial and territorial levels of government.

2.2 US CAV Deployment Context

On December 31, 2020, the US Department of Transportation's Federal Highway Administration (FHWA) awarded ten Advanced Transportation and Congestion Management Technologies Deployment (ATCMTD) grants to projects using intelligent transportation systems (ITS) technologies to improve mobility and safety and support vehicle connectivity. Many of these projects involve infrastructure components [4]. For example, the Metro Government of Nashville & Davidson County in Tennessee (Public Works Department) are working on an improvement to the transit headways and congestion management by introducing improved infrastructure that can enable CAVs to manoeuvre in traffic more effectively. The University of Michigan is looking to outfit intersections with cameras, radar, and infrared sensors in order to capture what is moving in the area, at what location, speed, and heading – everything from cars to pedestrians. That information can be instantaneously sent to connected vehicles in the vicinity triggering onboard warnings when cars are in dangerous situations. Digital infrastructure elements, such as sensors placed at intersections, can provide additional data to those vehicles wirelessly, enhancing their capacity to detect dangers.

In addition, there have also been several National Cooperative Highway Research Program (NCHRP) research projects funded under the Transportation Research Board. For example, NCHRP 20-102(15) is looking at the impacts of CAV technologies on the highway infrastructure [5]. The objective of this research is to produce guidance for state and local transportation agencies in evaluating and – if necessary – adapting their standards and practices for roadway and intelligent transportation system designs (including traffic control devices) and related maintenance and operations to reflect the deployment of CAV technologies. There is also NCHRP 20-102(24) which is anticipating evaluating infrastructure modifications that can improve the operational domain of autonomous vehicles (AVs) [6]. The study notes that in order to achieve a smoother transition to CAV transportation, state and local agencies must understand how and when traditional highway and street infrastructure may be affected and the impacts this could have on design, operations, maintenance, and policy. Much of the physical infrastructure work guiding these projects has been guided by the MUTCD, which provides minimum standards and guidance to ensure uniformity of traffic control devices across the US and Canada, respectively. The use of uniform traffic control devices (messages, locations, sizes, shapes, and colors) helps reduce crashes and congestion, and improves the efficiency of the surface transportation system. All public agencies and owners of private roads open to public travel across the nation rely on the MUTCD to bring uniformity to the roadway [8].

When considering future CAV deployment opportunities in the United States, much like in the previous Canadian case, there are a number of unique features that pose novel challenges when developing a unified framework for North American CAV operations. For example, the geographically dispersed cities with broader urban sprawl, higher speed limits, and heavy dependency on the personal automobile for mobility pose unique challenges for CAVs standards development and integration with Canada. As an initial step in bridging this gap, SAE International has been developing an automated driving system (ADS) roadmap to help industry members and regulators better understand the CAV standard landscape and visualize connected activities as well as gaps in the existing standards ecosystem.

2.3 International CAV Deployment

Initial efforts exploring how infrastructure can improve CAV deployment and operations have been demonstrated internationally. One example is the MAVEN (Managing Automated Vehicles Enhances Networks) project under the European Horizon 2020 effort. This project is developing infrastructure-assisted traffic management solutions for CAVs at signalized cooperative intersections (CIs) for increasing urban efficiency and safety. CIs exchange information with CAVs, which consider it in their perception and planning logic. To ensure backward compatibility, MAVEN extends the sensing capabilities of CAVs by providing Signal Phase and Timing (SPaT) information along with MAP (geometric data on intersections and roadway lanes) messages related to traffic light signalling. MAVEN has demonstrated that lane change and lane-specific speed advisories can be delivered with a novel vehicle-to-everything (V2X) service and a dedicated SPaT/MAP profiling, respectively. This enables CIs to more granularly and efficiently serve the demands of CAVs at intersections.

Another similar effort is the AutoNet2030 project. This effort has a similar vision and set of objectives to MAVEN: performing research into understanding how infrastructure can enable CAVs. Today, most developments target standalone AVs, which are capable of sensing the surroundings and controlling the vehicle under nominal conditions with the need for human intervention. The inherent drawback of this solution is the lack of coordination among vehicles and the limited range of sensors, which results in suboptimal performance. Vehicle-to-infrastructure communication (V2I) overcomes these drawbacks by increasing the planning horizon of AVs and enabling various cooperative driving automation (CDA) features.

2.4 The Role of Infrastructure

Infrastructure plays a critical role in the effectiveness of CAVs for several reasons. One of the most critical concerns involves the ability to sense and appropriately interpret physical infrastructure components like road signs or markings. The ability for AVs to identify infrastructure components or contextualize the meaning of the surrounding environment as part of the data fusion and evaluation process depends on things like the quality, visibility, colour, and degradation of infrastructure elements. Just as conditions like signs occluded by vegetation or snowfall can make it harder for humans to drive, so too can these infrastructure-related challenges make the dynamic driving task more challenging.

With regard to physical infrastructure, we note that only 41% of US roads meet the requirements for a “good ride”, as scored according to the International Roughness Index [9]. The most important factor for driving automation was found to be clear lane markings. In addition, mapping software requires highly accurate data and measurements along with clear markings to function optimally. For complex intersections, CAVs may need to record dimensions down to the decimeter level. Roads continually deteriorate and road markers fade; the physical structure of the intersection is constantly changing. Even minute alterations could impede the functioning of CAVs.

Separately, with regards to digital infrastructure, there are several opportunities to bring about higher levels of driving automation with CAVs in a safe and secure manner. Applications running on a combination of cloud and edge architectures and supported by a variety of communication platforms – including satellite, Wi-Fi, 4G LTE, 5G, and cellular V2X to name a few – can provide low-latency communications to/from vehicles that can support with different aspects of the automated vehicle stack involving recognition, prediction, planning, situational awareness, and control. These communications are designed and operated not only to support the onboard blocks of the automated driving platform but also the needs of a mixed traffic flow, which includes connected and non-connected vehicles and AVs with different levels of automation. This infrastructure has the potential to offer data security, wireless coverage, and wide interoperability. It can be flexible and adapt to urban and interurban use cases, congestion and different traffic composition with different levels of penetration of CAVs mixed with platooning and cooperative driving.

For the future, shared and automated mobility services provided by fleets – one of the first SAE Level 4 ADS use cases – will rely on digital infrastructure to dispatch, manage, and service CAVs. Regardless of whether private or public entities decide to develop support facilities, there is a need for fleet companies to make use of infrastructure that would allow the vehicles to be stored in central locations assuming a ride-hailing business model approach. The facility placement must be determined carefully to avoid disrupting the urban environment and negatively impacting health, traffic, and civic life. It is possible to repurpose existing infrastructure, but there will undoubtedly be costs associated with the facilities such as rent, labour, and creation of charging infrastructure for electric vehicles (EVs). It is important to start evaluating how support facilities can be managed and maintained as CAVs start to be used more widely in urban areas.

3. Methods

The development of a CAV code framework was guided by literature and a diverse group of industry experts. The following documents were used to evaluate the context behind the framework topic areas and to understand how the topic areas were evaluated under prior research:

- CSA Group, “Connected and Automated Vehicle Technologies – Insights for Codes and Standards in Canada” [1]
- SAE ADS Standards Roadmap[1]
- British Standards Institute, “CAV Standards Roadmap” [10]
- British Standards institute, “PD ISO/TR 4609 – Report on Standardization Prospective for Automated Vehicles (RoSPAV)” [11]

These documents helped identify which standards were relevant towards developing a digital and physical infrastructure framework for CAVs. Subsequently, a literature review was performed to identify additional applicable standards and research. From each of the literature sources reviewed, the relevant specifications or findings that pertain to developing a framework for a multi-national code were identified. For example, one of the literature sources identified in CSA Group’s report cited above [1] was the US Manual on Uniform Traffic Control Devices or MUTCD [8]. This document provides varying levels of specifications depending on the physical infrastructure component of interest. It uses different types of specification statements to delineate between requirements and specifications versus guidelines or general principles. Each of these details were carefully tabulated in an Excel sheet that identifies the relevant standard, specification, and applicability towards developing a code. Finally, a detailed interview process was conducted to validate the results and identify additional relevant literature sources and specifications that should be included as part of the framework.

[1] Access to this resource is only available through SAE. For inquiries, please contact Edward Straub, SAE, at: Edward.Straub@sae.org.

3.1 Literature Review

A comprehensive review of the CAV standards landscape was performed, comparing the results uncovered during the research into several recent reports that have performed similar analyses. The following sections provide an overview of the relevant topic areas for this framework, including the scope of the specific section, the applicable literature, and any relevant stakeholder feedback that is pertinent for a given literature source. The review began with the relevant topic area's definition, which provided a foundation to identify what elements of certain pieces of infrastructure were applicable to a given subtopic. The definitions evaluated in this document are taken from sources that include many different and relevant standards within this space. After identifying the appropriate definition, subtopics from a range of ongoing and existing standards development efforts were collected and organized into categories. In addition, expert feedback gathered during the stakeholder interviews was applied to confirm the topic area's definition and the relevant subtopic categories.

Traditionally, an infrastructure can be thought of as a series of components that can be built, touched, enabled, and disabled to form interrelated, dependent systems that deliver needed commodities and services to society as a means of facilitating economic productivity and promoting a standard of living. Jeffrey Fulmer defines infrastructure as "components of interrelated systems providing commodities and services essential to enable, sustain, or enhance societal living conditions"[2]. Generally, engineers use the term infrastructure to describe fixed assets that are in the form of a large network. However, the traditional definition of infrastructure can be extended to include the definition of "critical infrastructure (CI)" provided by Public Safety Canada [12], which defines it as "processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. CI can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of CI could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence". Using this context, this document defines infrastructure as road or traffic components that provide a commodity or service for road users, with infrastructure being subdivided into digital infrastructure, physical infrastructure, and cybersecurity and data security/privacy subcategories. Each of these subcategories will be described in greater depth along with their subcomponents in the following sections.

3.2 Stakeholder Interviews

More than half a dozen key experts with advanced knowledge and expertise in the framework's topic areas of interest were identified to be interviewed for their perspectives on existing standards and gaps. Experts ranged from cybersecurity and digital communications developers to leaders in physical infrastructure standards development. Individual, one-on-one interviews were scheduled with the domain experts and questions were asked pertaining to the relevant standards within the individual's domain of expertise. Many of the interview questions were focused on specific standards or gaps that had already been identified and could be reviewed with the interviewees. After each discussion, relevant findings were analyzed and used as the basis for further research in order to better understand the premise and evaluate its application to the framework. Many of the findings have been used to identify additional gaps within the digital and physical infrastructure domains beyond those identified as part of the literature review. A list of the questions asked of the stakeholders may be found in Appendix A.

4. Results and Discussion

This section discusses the findings for each of the three major topic areas covered by this study: digital infrastructure, physical infrastructure, and cybersecurity and data security/privacy. Each section is followed by multiple subsections describing features and aspects of the main topic area, as well as gaps in standardization, where applicable.

[2] Fulmer, Jeffrey (2009). "What in the world is infrastructure?". PEI Infrastructure Investor. Available : https://30kwe1si3or29z2y020bgbet-wpengine.netdna-ssl.com/wp-content/uploads/2018/03/what-in-the-world-is-infrastructure.pdf

4.1 Digital Infrastructure

Transportation infrastructure has long been recognized to comprise a complex, interactive, and interdependent system. Like other such complex systems, management thereof is greatly enabled and enhanced through the application of a digital infrastructure alongside and overlaying a physical infrastructure. A digital infrastructure employed in this manner enables the collection of real-time performance data, as well as the dissemination of data, including instructional information, that can improve both safety and mobility (throughput), especially at intersections, highway interchanges, construction and post-incident sites, and other locations known to be prone to safety risks and/or traffic congestion.

A digital infrastructure is any hardware or service that provides information technology capabilities. This can include anything from networks and telecommunications to data centres and cloud computing. A digital infrastructure includes any infrastructure component that sends or receives data to/from another component or road user. Some of the messages exchanged are carried over a communication interface. For this framework, a digital infrastructure encompasses the hardware (e.g., road furniture) that can collect data from the environment, the hardware that communicates with CAVs using V2X messages on the ITS spectrum[3], as well as other services, some in which data are sent to CAVs, and others in which data are sent by CAVs. More specifically, the aspects are:

- Roadway sensors
- Communications with road infrastructure
- GNSS positioning and timing
- High-definition mapping

4.1.1 Roadway Sensors

Roadway sensors that are installed along the roadside are used to collect and convey traffic or traveller information to road users and connected management equipment, such as a traffic signal controller or a traffic management centre (including fleet operations). Roadway sensors are an effective part of any intelligent traffic surveillance system and provide monitoring capabilities to track traffic and weather conditions across a road network or region. Sensors may be installed in, on, or above the roadway to obtain the appropriate location, condition, and time coverage. This may include inductive loops, non-intrusive traffic and weather detection devices, video cameras and video image processing. (Note: Roadside sensors do not include sensors that are installed on dynamic objects or on fixed objects that are temporarily installed on the roadside.)

Gaps

Edge/cloud systems able to ingest and manage large amounts of connected and automated vehicle (CAV) data collected by roadway sensors and the governance of such systems have not yet been specified or standardized. These will need to include a specification for maximum latency for edge computers for processing data collected by roadway sensors and dispatching real-time signals to traffic participants.

4.1.2 Roadside Communications Infrastructure

A roadside communications infrastructure is deployed to support various safety and operational functions used by infrastructure owners/operators (IOOs) to improve the safety and efficiency of roadways. It consists of equipment known as roadside units (RSUs) mounted on traffic signal poles or other structures, equipped with a wireless interface that enables the exchange of messages with vehicles using the ITS spectrum. This type of communication is also known in the literature as I2V/V2I (infrastructure to vehicle/vehicle to infrastructure) communications. All CAV to RSU communications over the ITS spectrum are

[3] "ITS spectrum" in our usage refers generally to any wireless spectrum allocated specifically for transportation use. This includes, but is not limited to, the 5.850-5.925 GHz Band, which was associated with dedicated short-range communications (DSRC) wireless communications protocol 80211.p. However, in a reversal of long-standing policy, the US Federal Communications Commission reduced this part of the ITS spectrum allocation from 75 MHz to 30 MHz, reallocating the lower 45MHz to unlicenced Wi-Fi users, and specifying that remaining 30 MHz be dedicated for cellular V2X, rather than DSRC. Canada, which had previously reserved the 5.850-5.925 GHz Band for DSRC in harmony with the US, so far has not changed its spectrum allocation rules.

within the scope of the infrastructure framework, with the exception of tolling and vehicle-to-grid (V2G) communications, as they do not use the ITS spectrum and they are not specific to CAVs.

In order to facilitate improved safety and mobility, RSUs broadcast periodic and episodic messages for nearby vehicles that are able to receive them. The RSUs may be the source of the data sent, or they may have obtained the data from other devices such as real-time kinematic or Radio Technical Commission for Maritime Services (RTCM) source, or traffic management backend systems such as probe data management and road weather management. RSUs may also receive messages sent by vehicles, to capture and send them to either a traffic management system or a backend server on the network.

Gaps

To date, there is a lack of standardization for RSU-coordinated messages to facilitate advanced manoeuvres for CAVs at intersection crossings and lane merging/change operations for CAVs. However, these appear to be within the purview of the new Cooperative Driving Automation (CDA) Committee established in December 2020 by SAE.

4.1.2.1 Security Credential Management System (SCMS) to Support RSU Communications

Within the area of communications infrastructure (that is, RSUs), an important and self-contained aspect regards the infrastructure that supports the security of such communications. An infrastructure-based security credential management system (SCMS) is responsible for generating and delivering the digital certificates that are used in the message verification process for messages exchanged between vehicles or between vehicles and infrastructure (RSUs). The SCMS can also revoke certificates that should no longer be trusted by placing them on a certificate revocation list that the SCMS distributes to all systems. This security management system is applicable for North American V2X communication deployments, and it deals with issuing certificates conformant to IEEE 1609.2 (Appendix B.1) to RSUs and to onboard units (which are part of CAVs).

The SCMS is a network of specified functions that work together to achieve the goal of issuing certificates to secure vehicle-to-vehicle (V2V) and V2I messages between vehicles and between vehicle and infrastructure, while preserving user privacy. As CAV technology proliferates, it is expected to also support vehicle-to-device/device-to-vehicle (V2D/D2V) communications, such as communications devices potentially carried by vulnerable road users. Together, V2V, V2I, I2V, V2D, and D2V are referred to as V2X.

Gaps

Currently, the SCMS lacks a legally sanctioned governance framework and authority, which it requires to issue and enforce SCMS rules of operation. This will be particularly important for maintaining cross-border agreements between Canada and the US.

4.1.2.2 First Responder Communications

Among communications needs serviced by the ITS spectrum are communications with and between first responders, including police, fire and rescue, and medical emergency vehicles and personnel. First responder activities are greatly facilitated by communications technology, which enables the deployment of specialized teams and equipment tailored to specific incidents and their exigent circumstances. Such a tailored response capability improves the chances of survival by crash victims.

First responder communications are defined as a subcategory of roadside communications that supports emergency vehicle response and operations. All V2I communications for emergency vehicles are in the scope of the infrastructure framework. First responder activities differ for CAVs that can be supported via existing communication protocols for this purpose. SAE J2735 currently defines DSRC message formats for use with emergency vehicles. The existing standard supports communication (on the ITS spectrum) between emergency vehicles and RSUs, to influence the traffic signal, namely the signal request message (SRM). The RSU responds with a signal status message (SSM). This messaging can be used for emergency CAVs.

Gaps

There is a need to identify potential interactions between first responders and driverless-capable ADS-operated vehicles, and to develop guidance for these interactions. This may require developing first responder scenario data sets for ADS developers to use in training their algorithms to perceive first responders and determine correct responses (e.g., recognize emergency vehicle lights, sirens, perform manoeuvres). Additionally, there are opportunities to develop beyond DSRC communication standards for emergency CAVs.

4.1.3 GNSS Positioning and Timing

The ability to geolocate is essential to the safe and efficient operation of CAVs. One of the primary sources of geolocation data is the Global Navigation Satellite System (GNSS), of which the Global Positioning System (GPS) is a prevalent form. GPS data are generally differentially corrected using grounded base stations to achieve an accuracy within several centimetres of ground truth. Location/positioning data are further enhanced by the use of high-definition (HD) maps, as well as inertial sensing, which is needed to compensate for the temporary interruption of GPS signals, such as while passing through tunnels or through “urban canyons”.

GNSS is a navigation system that uses satellites, a receiver, and algorithms to synchronize location, velocity, and time data for air, sea, and land travel. All GNSS aspects are relevant to CAVs, which rely heavily on geolocation for navigation, as well as maintaining an operational design domain (ODD) and updating high-definition digital maps. GNSS comprises the technology and communication protocols associated with accurate worldwide navigational systems based on the reception of signals from an array of orbiting satellites. This includes onboard vehicle hardware as well as additional land infrastructures used to enhance positional accuracy, for example, by issuing real-time corrections.

Gaps

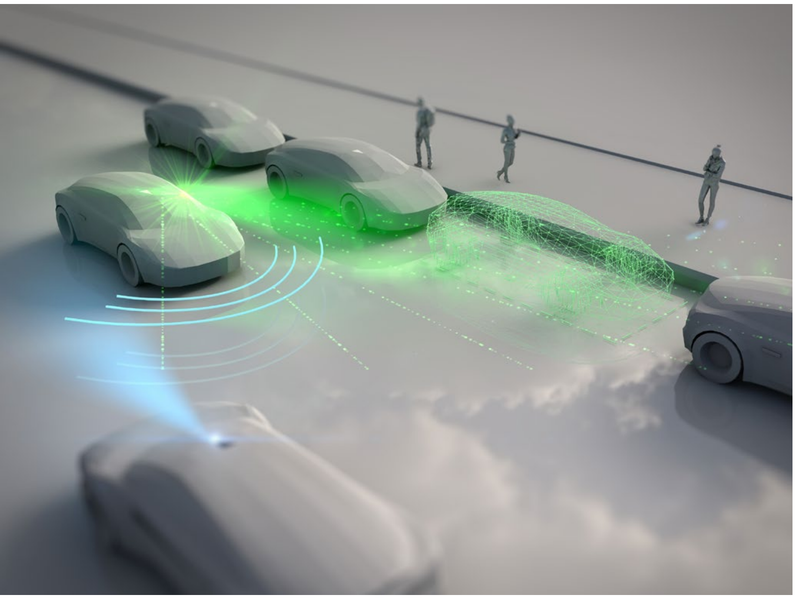
A key enabler of ADS technology is the provision of accurate geolocation data on an ongoing basis. Such geolocation data are provided by the GNSS, with GPS being the signal system most widely used today. However, GPS signals are unable to penetrate certain environments, such as urban canyons (as well as actual canyons), tunnels, and roadways covered by a dense arboreal canopy. CAVs may temporarily compensate for lack of GPS signals with inertial sensors, but such sensors accumulate significant errors over time, and thus are not reliable when areas of GPS signal obscuration are large. As such, there is a need for physical characteristics, and to assess the extent to which such road segments exceed ADS-operated vehicles’ ability to adequately compensate by using inertial sensing.

Additionally, GNSS also relies in large measure on earth-bound base stations for enabling GPS signal differential correction to improve accuracy. As such, there is a need for a standard that establishes the location and frequency of such base stations to support the needs of ADS-operated vehicles.

4.1.4 High-Definition Mapping

High-definition (HD) maps provide near-real-time roadway information in sematic detail sufficient to support path planning and execution by an ADS-operated vehicle. According to the ride-sharing company, Lyft, HD maps consist of five layers of information, four of which build upon information stored in existing standard definition maps. These layers consist of the base map, the geometric map, the semantic map, map priors, and real-time knowledge.

1. The base map layer contains much of the same information found in traditional 2D maps, including streets, parcels, boundaries (country, county, city boundaries), shaded relief of a digital elevation model, waterways, and aerial or satellite imagery.
2. The geometric map layer contains highly detailed 3D information of the world. Raw sensor data from lidar, various cameras, GPS, and inertial measurement units (IMUs) are processed using simultaneous localization and mapping (SLAM) algorithms to develop a 3D view of a mapped area which can then be used for onboard calculation and inference.
3. The semantic map layer builds on the geometric map layer by adding semantic objects. Various



> "HD maps are essential for the safe operation of CAVs... [They] are three-dimensional representations of the real world... [and] allow a CAV to understand its location, its surrounding physical environment, and the rules of the road."

2D and 3D traffic objects, including lane boundaries, intersections, crosswalks, parking spots, stop signs, and traffic lights that are used for driving safely, are stored in this layer and used in conjunction with the geometric map layer to provide contextual information about the 3D operational environment.

4. The map priors layer contains information about dynamic map elements. Information stored in this layer can contain both geometric and semantic data. For example, historical traffic light orders at intersections and the amount of time spent in each state are encoded in the map priors layer.
5. The real-time layer is the apex layer in the HD map. It is the only layer in the map designed to be read/write capable and updated while the map is in use. It contains real-time traffic information captured by the operating AV such as traffic congestion, observed driving speeds, and accident/construction zones. The real-time layer is designed to support gathering and sharing of information between CAVs.

HD maps are essential for the safe operation of CAVs. The maps are not the traditional two-dimensional paper or GPS versions we are familiar with, but rather are three-dimensional representations of the real world. HD maps, which come within centimetres of accuracy, allow a CAV to understand its location, its surrounding physical environment, and the rules of the road. Due to the complexity and data-intensity of HD maps, CAVs require extensive onboard computing power to quickly collect, store, process, and transmit this tremendous amount of data.

Gaps

Guidelines are needed for safety- and performance-related data sharing, especially from temporary traffic zones (e.g., work zones, incident scenes). This should start with identifying needs (e.g., sharing for better common operational picture and interoperability) so that the data can be standardized and show up in the same format on all HD maps.

4.2 Physical Infrastructure

The physical infrastructure for road transportation serves the tangible needs of road traffic by providing roadways, bridges, tunnels, and junctions that facilitate safe and efficient travel using motorized vehicles of various weights and sizes. It includes physical and signalized traffic control devices, including pavement markings, signage, signalized traffic lights, and crosswalks to accommodate pedestrians.

The physical infrastructure provides essential services to road users and consists of tangible objects that do not involve the transfer of data. In contrast, the digital infrastructure provides only data-transfer-related services and involves objects that directly send traffic-relevant data to road users. For example, lane markings do not send data to a road user. Road users sense the lane markings using sensors, but the lane marking does not provide information to the road user on its width, colour, shape, or length.

This physical infrastructure section was developed by identifying infrastructure components that exist in relevant standards and literature sources. The following components were identified as satisfying these criteria:

1. Intersections
2. Crosswalks
3. Traffic control devices
   a. Road surface markings
   b. Signals
   c. Signage
4. Roads
   a. Geometry
   b. Sight distance
   c. Design elements
5. Architecture (bridges, tunnels)
6. Barriers and work zone equipment
7. Accessibility applicable documentation

Two overarching standards applicable in Canada and the US are the Manual on Uniform Traffic Control Devices for Canada (MUTCDC) [7] and the US Manual on Uniform Traffic Control Devices (MUTCD) [8]. The MUTCD and MUTCDC provide minimum standards and guidance to ensure uniformity of traffic control devices across the US and Canada, respectively. The use of uniform traffic control devices (messages, locations, sizes, shapes, and colors) helps reduce crashes and congestion, and improves the efficiency of the surface transportation system. All public agencies and owners of private roads open to public travel across the nation rely on the MUTCD and MUTCDC to bring uniformity to the roadway; however, it is important to note that compliance with this guidance is voluntary, rather than mandatory, although in the US, the MUTCD compliance may be incentivized through federal highway funding.

4.2.1 Intersections

Roadway intersections allow roadway travellers to change direction in order to reach their destinations. They are of particular interest for IOOs, both because of the challenges they present in terms of crash risk and interaction with vulnerable road users (VRUs – e.g., pedestrians, pedal cyclists, wheelchair users) and the opportunities they present in terms of collecting and disseminating data through the use of the digital infrastructure that can in turn be used to improve safety and throughput.

The American Association of State Highway and Transportation Officials (AASHTO) defines an intersection as the general area where two or more highways join or cross, including the roadway and roadside facilities for traffic movements within the area [13]. More specifically, an intersection can be considered an at-grade junction where two or more roads or streets meet or cross. Intersections may be classified by number of road segments conjoined, traffic controls, or lane design. For Canadian provinces and territories, intersections are defined based on the local transportation authority. For example, Alberta defines an intersection as a junction where two or more roadways meet, creating a possible conflict between vehicles on those roadways and with pedestrians crossing those roadways. Intersections may be controlled by traffic signs, traffic signal lights, or both. Intersections not controlled by signs or signals are controlled by rules and regulations [14].

Intersections play a vital role in the traffic network but are also the most hazardous locations in terms of crash risk, accounting for approximately 40% of the crashes that occurred in the US in 2008 [15]. Additionally, about 96% of the intersection-related crashes involved driver errors, such as inadequate surveillance, false assumption of other’s action, and turning with obstructed view [16]. In addition to reducing crashes, intersection management is critical for energy efficiency and fuel consumption. Fuel consumed by vehicles makes up almost 75% of all transportation energy used [17]. Moreover, high gasoline consumption at intersections worsens air quality in urban areas, making them potentially dangerous to human health. According to the US Department of Transportation, it is anticipated that by 2040, up to 80% of intersections in the US may be equipped to communicate with vehicles [18].

Of note, the Institute of Transportation Engineers (ITE) is currently working on developing and publishing a standard (or a Recommended Practice) that defines the key capabilities and interfaces a connected intersection must support; however, it has yet to be released publicly at the time of writing this report.

Gaps

Thus far, CAV standards have focused primarily on specifications between physical infrastructure and road users at intersections. However, these specifications do not provide requirements to infrastructure developers on guidelines or recommendations for developing or testing physical infrastructure components to accommodate CAVs at intersections. Most specifications for intersections assume mostly human drivers and do not account for automated driving systems with unique software perception and planning stacks. Specifications are needed to define requirements for specific physical infrastructure components at intersections, as well as guidelines that provide best practices for component placement, connection types, and consistency across physical infrastructure vendors.

One of the most significant gaps for intersections involving physical infrastructure is defining infrastructure standards and developing requirements and test procedures for vehicle-to-infrastructure communication [19]. There are standards for specific message types and how they can be communicated (ISO 19091 [20]), but there is a gap in understanding how data can be fused at an intersection so that perception data from various sources can be amalgamated to help prevent crashes. Additionally, opportunities exist to improve standards around data quality, response times, and responsibilities during exchanges (i.e., handshakes that establish the protocols of a two-way communication).

4.2.2 Crosswalks

Crosswalks facilitate safer street crossing by VRUs by serving as designated areas for this purpose that impose specific yield obligations on the part of motorized vehicle operators. Crosswalks are always designated by a minimum of pavement markings, but they may also include dedicated signalling devices, including ones that feature traffic signal phase and timing devices to prioritize the crosswalk for VRU traffic.

The US Federal Highway Administration defines a crosswalk as follows: a) That part of a roadway at an intersection included within the connections of the lateral lines of the sidewalks on opposite sides of the highway measured from the curbs, or in the absence of curbs, from the edges of the traversable roadway; and in the absence of a sidewalk on one side of the roadway, the part of a roadway included within the extension of the lateral lines of the existing sidewalk at right angles to the centerline, or b) Any portion of a roadway distinctly indicated for pedestrian crossing by lines or other markings on the surface [21].

The British Columbia *Motor Vehicle Act* provides a similar definition, minus addressing the presence of curbs and intersection/roadway geometry [22].

Studies have been conducted to evaluate relationships among AV driving behaviour, crosswalk type, pedestrians' trust in the AVs, and trusting behaviour [29]. There is a significant amount of research evaluating how AVs can broadcast and appropriately communicate their intent to pedestrians [25]-[30]. Moreover, several studies have evaluated how varying crosswalk types have affected the decision of a pedestrian to cross [31]. More broadly speaking, researchers at York University, Amir Rasouli and John Tsotsos, have developed a dendogram to understand the various factors that influence VRUs crossing at crosswalks, including the social factors, physical infrastructure, context for crossing, dynamic factors, vehicle and pedestrian characteristics or attributes, and demographics of different VRUs [24]. This research has led to the development of a number of standards relevant to crosswalks in an effort to generate functional safety requirements and recommendations for crosswalk implementation with respect to CAVs.

Gaps

One of the most prominent gaps yet to be addressed is understanding how different types of crosswalk markings affect CAVs. Sensing and perception algorithms must be able to appropriately detect and react to different crosswalk markings without confusing them for other types of road surface markings (such as lane markings). In many cities, crosswalk markings look very similar to fire lane guidance warnings or warnings not to enter a specific road surface area while stopped at a traffic signal. With the difficulty that humans experience in understanding these markings, it may be even more challenging for CAVs to appropriately determine a crosswalk and subsequently react.

" ... novel crosswalk designs pose apparent problems for AVs, which must be "trained" to recognize every novel crosswalk design."

In addition, some municipalities are deploying novel or theme-based pedestrian crosswalk markings, adding colour and new designs, or making them appear to be three-dimensional. Such novel crosswalk designs pose apparent problems for AVs, which must be "trained" to recognize every novel crosswalk design.

How VRUs communicate and coordinate with other road users at a crosswalk is another gap in this space. There is plenty of research to build from, but standards are required to help ensure consistency among multiple types of crosswalks and how VRUs are expected to coordinate at crosswalks with varying markings, lines, colours, and communication protocols. Especially for those persons with disabilities that may require some sort of visual or cognitive assistance to know when it is safe to cross, or who might require longer cross times, standards can help ensure all types of VRUs are able to effectively cross in a safe manner.

4.2.3 Traffic Control Devices

Traffic control devices are used to regulate the flow of traffic and the movements of particular traffic participants in real time. They establish rights-of-way and yield rules at junctions, merge points and intersections, and they regulate the speed and direction of traffic along all public roadways.

Traffic control devices include signs, signals, pavement markings, and other devices placed along highways and streets to provide for the safe and efficient movement of all road users. These devices are placed in key locations to guide and regulate traffic movement, control vehicle speeds, and warn of potentially hazardous conditions. Traffic control devices also provide important information to users about detours and traffic delays. Traffic control devices that appear before an intersection and at an intersection are of particular importance.

4.2.3.1 Road Surface Markings

Road surface markings include any device or material that is applied to a road surface in order to convey regulatory information to road users, including VRUs. The MUTCD provides examples and definitions for specific types of markings, rather than for markings in general. One example includes lane line markings, defined as white pavement marking lines that delineate the separation of traffic lanes that have the same direction of travel on a roadway [8].

There may be markings on a road surface that were made accidentally or to convey information that is not authorized for traffic control purposes by a local or state authority. These types of road markings are not included in the scope of the road surface markings because there is no way to develop standards for road markings that are placed accidentally or extrajudicially.

Road surface markings are critical for ADS and advanced driver assistance system (ADAS) because the human and the ADS must be able to appropriately perceive the marking, interpret it correctly, fuse the data with other environmental parameters, and then make a decision accounting for the marking and its meaning. Several CEOs and organizations have stressed the importance of road markings:

- Elon Musk during a Tesla Innovation Conference: "We really need better lane markings in California." [32]
- Lex Kerssemakers, CEO, Volvo Car Group: "It can't find the lane markings! You need to paint the bloody roads here!" when referring to U.S. roads. [33]
- EuroRAP and Euro NCAP: "Like the human eye, the technology cannot work effectively if it cannot see the road markings and traffic signs, if they are worn out or hidden, or if they are confusing." [34]

Clearly visible and unambiguous road markings support the human driver and the CAV in navigating roadways. Sensors are an integral component of ADAS and ADS, and different types of sensors have separate requirements for road surface markings, for example, light detection and ranging (LIDAR) sensing versus a camera.

Gaps

Current road surface marking standards only specify functionality within a human's visual range. Innovative road surface markings are required to provide information outside of the visual range, and this requires new specifications and guidelines. Many OE (original equipment) vehicle manufacturers use cameras to identify lane markings, which is critical for lane-centring features. While the quality of lane markings is critical, adverse weather conditions and worn-out markings pose great challenges to cameras even with high-quality markings.

4.2.3.2 Signals

Traffic control signals use lights, usually placed in a vertical pattern of red, yellow, and green descending in order from the top of the traffic signal housing. These lights signify specific information/instruction to users travelling in lanes subject to them (i.e., red: you must stop; yellow: the light is about to turn red; and green: you can proceed through the traffic zone). Some traffic control signals, however, do not employ the red-yellow-green information just described, but rather may flash red or yellow to indicate danger or caution, such as at railway crossings or crosswalks. Lighted signals are also frequently employed at work sites/construction zones to warn passing traffic of the presence of workers and work vehicles in the vicinity of the roadway.

A traffic control signal (or traffic signal) is defined as any highway traffic signal by which traffic is alternately directed to stop and permitted to proceed [8]. Within this definition, traffic is defined to include pedestrians, bicyclists, ridden or herded animals, vehicles, streetcars, and other conveyances either singularly or together while using any highway for purposes of travel. One of the key aspects of the term for a traffic signal is that the signal controls the flow of traffic and determines when road users must stop and when they can proceed. Common traffic lights are one of the most common signals, but there are other signals included in this definition such as flashing signals near crosswalks and fire stations or crossing gates near railroad crossings. These physical infrastructure elements are used to convey variable messages rather than specify a single regulatory requirement like a sign. For example, closed and flashing crossing gates near railroads are conveying the message that a road user should not cross over the railroad tracks because a train is either about to cross the tracks near the road's intersection or that the train is still in the process of crossing.

There are many benefits to coordinating between CAVs and traffic signals. As noted in [35], some of the potential advantages include crash frequency or severity reduction, travel time optimization, and energy efficiency improvements. To realize these benefits, there is a large body of research that evaluates varying levels of signal interaction and feedback versus feedforward loops in order to understand the best approaches to connection depending on the intersection and level of automation for a given vehicle. These include:

- **Actuated signal control –** determine signal changes based on traffic density.
- **Platoon-based signal control –** provide signal priorities for platoons.
- **Planning signal control –** pre-program signals based on known characteristics of an operational design domain (ODD).
- **Signal-vehicle co-control –** allow CAVs to provide messages to traffic signals that indicate a need to proceed or stop.

Early CAV deployments have demonstrated transit signal priority [36], emergency vehicle preemption [37], and heavy truck signal priority [38]. This has led to an emergence of standards providing specific protocols and implementation practices for traffic signal coordination with CAVs.

Gaps

We have identified two areas where gaps exist with regard to current standards: 1) data acquisition, storage, and management, and 2) application harmonization.

Data acquisition, storage, and management – With an abundance of traffic signals, there will be a tremendous amount of data involved as each traffic signal has requirements to acquire the data, cleanse it, store it, transfer it, and disseminate it to the appropriate road users. This type of big data use case will require new sets of standards to identify how traffic signals can implement methodologies to maintain data using standard elements and place data within a cloud services architecture that organizations are able to access. Different levels and types of CAVs will require unique data inputs with different types of information and different ways to access that information. Although formats such as the JSON or ASN.1 protocols can be used, standards still need to specify what type of information should be provided and outline the exact dependencies or assumptions for a given traffic signal.

Application harmonization – There are numerous efforts underway evaluating different signalized intersection applications. In order to develop an effective standard that outlines the exact protocols and methods to use for an application, manufacturers, infrastructure owners and operators, and researchers need to agree on the best techniques to use for a specific application. There are some applications that have been fully developed and agreed upon by the community that are included in SAE J2945/B (Appendix B), but further applications will not only require more research but also collaboration between different stakeholders to determine the best approaches.

4.2.3.3 Signage

Traffic signs are usually static and convey a single regulation, instruction, warning, or status, such as applicable speed limit, the fact that a lane will end in X distance, the possibility of rock slides in the area, or the imminent presence of a work or school zone. Signs are designed for human readability, and may contain words, symbols, or a combination thereof.

A traffic sign is defined as any traffic control device that is intended to communicate specific information to road users through a word, symbol, or arrow legend [8]. An important consideration for traffic signs is that signs do not include highway traffic signals, pavement markings, delineators, or channelization devices. Although there may be pavement markings that use words or symbols to communicate relevant traffic information, these elements are captured in the road surface markings and traffic control devices sections. Signs are strictly limited to physical infrastructure components and provide a notice that is publicly displayed giving information or instructions in a written or symbolic form to road users.

The Federal Highway Administration has developed the Standard Highway Signs and Markings handbook [8] to provide details for different types of signs in terms of their dimensions, colour, font, and shape. This handbook is the primary guiding document for infrastructure owners and operators in the US looking to implement signs that have been well-established. In terms of the placement of signs, MUTCD provides guidance for each type of sign in terms of the requirements for the geographical location and road network. Alternatively, road signs in Canada may conform to the Transportation Association of Canada's (TAC's) MUTCDC [7] for use in Canadian jurisdictions. Although it serves a similar role to the MUTCD, it has been independently developed and has a number of key differences with its American counterpart, most notably the inclusion of bilingual (English/French) signage for jurisdictions such as New Brunswick with significant anglophone and francophone populations, and a heavier reliance on symbols rather than text legends.

Humans are required to take an exam before receiving a driver's licence that analyzes their ability to comprehend the meaning of various traffic signs. During the driving portion of an exam, humans will similarly encounter traffic signs and are graded partially according to their ability to sense and appropriately respond to traffic signs. Until the introduction of automated vehicles, signs have been primarily designed for human sensing and perception. This is why most signs use extravagant colours, large bold fonts, and diverse shapes depending on the message that is being conveyed. One of the challenges for automated vehicles involves sensing and perception of signs, particularly when localities have varying signage, and even more so from country to country. Within some areas of the northern United States and in Canada, there are moose and snowmobile crossing signs [39]. In Washington state, there are volcano route signs to indicate best directions of travel in case of an eruption and corrosion to roads [40]. In Quebec, there are green signs with a camera pictured to indicate a red-light violation camera exists at a specific intersection [41]. The uniqueness and diversity of signs creates difficulties for automated systems that are trained using a specific subset of signs, which may not capture every relevant detail or sign that a vehicle might encounter [42].

Gaps

Use of standardized font type, size, message, and sign placement helps machine algorithms comprehend information. MUTCD provides guidelines on these parameters, but each locality has its own implementation, depending on the need. Areas with more sunlight where signs tend to fade may include lighter colours, which are cheaper to produce, whereas areas with more wind may need stronger physical materials to withstand heavy knots. Guidelines need to provide consistency in terms of how signs can be placed in common positions and areas, at similar heights, and use similar fonts for any text needed.

Adopting sign maintenance practices to keep signs clean and unobstructed by vegetation or other roadway infrastructure is also important – both for human drivers and ADS perception algorithms. This was identified in expert interviews and through many evaluations of current standards. Regardless of whether a sign is produced perfectly and placed in the exact right spot, there can still be environmental factors affecting an automated driving system's or even a human's ability to interpret the sign. Coordination is necessary with local department of transportation authorities to understand how maintenance can allow signs to be readable and seen according to the intended assumptions.

4.2.4 Roads

Roads present the most basic interface between motor vehicles and transportation infrastructure. Roads must be built to sustain motor vehicle traffic at regulated speeds and weather conditions (e.g., in terms of providing a sufficient coefficient of friction) and to withstand motor vehicle traffic spanning the range from motorcycles to oversize trucks and transport vehicles (e.g., in terms of structural and seasonal integrity). In addition, they must be built to specifications that also manage water runoff and provide protection from encroaching traffic, where needed. Since 1984, the American Association of State Highway and Transportation Officials (AASHTO) has published a comprehensive policy document commonly referred to as the Green Book [43], a compilation of specifications and guidelines for geometric design that serves as a primary reference providing design guidance on highways and streets. The Green Book is updated periodically to reflect updates to technology and regulations, as reflected in the 8th edition which is currently in development and being revised to reflect the need for increased flexibility in design with consideration to greater multimodal transportation adoption.

A road (also known as a roadway) is that portion of a highway improved, designed, or ordinarily used for vehicular travel and parking lanes, but exclusive of the sidewalk, berm, or shoulder even though such sidewalk, berm, or shoulder is used by persons riding bicycles or other human-powered vehicles. In the event a highway includes two or more separate roadways, the term roadway shall refer to any such roadway separately, but not to all such roadways collectively. Multiple roadways can be organized into a network that becomes a geographical arrangement of intersecting roadways.

The TAC publication, "Canadian Model Rules of the Road" [59], presents a generic set of traffic rules that road users should know and observe while using the road system. The model rules help practitioners understand how road users are expected to respond to various traffic control measures and other road situations. Among the various elements included are traffic control devices, passing, use of roadways, lanes, headway, right of way, pedestrians, turns, driver signals, special stops, speed restrictions, parking, alternate vehicles, bicycles, transit, and other provisions. As such, these are the core assumptions used to design physical infrastructure in Canada.

Gaps

None identified.

4.2.4.1 Road Geometry

Roadway geometry is an aspect of roadway design that, like coefficient of friction, must be tailored to the types of vehicles permitted on the roadway, as well as to applicable speed limits and line-of-sight visibility/critical distance. In many cases, speed limits are varied to accommodate tight curves, steep rises that limit visibility, or dips in a roadway necessitated by geography or human-built structures.

There is no exact definition for the geometry of a roadway, but there are several elements to a roadway geometry that can be defined. For example, a stretch of roadway could incorporate a route network. This could be any designated set of roadways and length of roadways on which a CAV may be designed to operate. The route network is a subset of the road network and can be thought of as a map of permissible roadways for a given CAV. SAE level 4 ADS-operated vehicles may have their ODD geography based on a set route network. Route networks are subsets of a larger road network and may be subsets within a geofenced area. The geometry also includes the superelevation and curvature of the roadway. Superelevation is an angle of elevation measured from the horizontal of the outside edge of a roadway on a horizontal curve. If vehicles are travelling more slowly than the original design speed for a high superelevation, lateral forces can pull the vehicle downslope creating a need for a vehicle to counter by steering upslope [43].

Vertical roadway curvature refers to crests or sags between tangent grades in roadways (i.e., hills or dips). Horizontal curvature refers to features connecting tangent horizontal (e.g., map view) roadways. Horizontal curvature (or curves) is described by radius and superelevation in roadway design. The road geometry for this document only applies directly to the road layout in terms of its size, dimensions, and length. Thus, any parameters affecting the road's dimensions are included. Other parameters that may affect the dimensions of the road (e.g., sight distance or grade) are discussed in other subsections.

Gaps

Current highway geometric designs are optimized for a human driver's perception and reaction time, and an average driver's eye height. Geometric design elements will need to be updated to account for CAV sensing and perception hardware. For example, in conventional vehicles, visibility at night depends on the vehicle's headlight height and the inclined angle of the headlight beam in calculating the length of sag vertical curves. However, for CAVs, LIDAR sensors operate similarly during day or night operations. Thus, new factors to consider for geometric designs include the height of the sensor above the roadway, the inclination of the vertical field of view of the LIDAR measured from the horizontal axis of the vehicle, and a LIDAR sensor's field of view [44].

In addition to recognizing and recording data relevant to the roadway geometry, CAVs also need to convert the data into a digital 3D model in real time. This allows the vehicle to accurately understand its current location and orient its position within the context of a larger area. However, CAV localization is difficult due to the large volumes of data required. Having an accurate road geometry description prior to performing the dynamic driving task is critical to allow localization to happen faster and produce more accurate measurements of proper speeds and turning angles. This allows the vehicle to derive kinematic and handling parameters from the road geometry prior to driving in the geometry.

4.2.4.2 Sight Distance

Providing adequate sight distance for motorists is critical for facilitating safe operation. Inadequate sight distance can result in crashes due to a driver's inability to brake in time to avoid collision with a late-appearing object in the roadway, such as upon cresting a steep hill.

Sight distance is the length of roadway ahead that is visible to the driver. The available sight distance on a roadway should be sufficiently long to enable a vehicle travelling at or a near the design speed to stop before reaching a stationary object in its path. Although greater lengths of visible roadway are desirable, the sight distance at every point along a roadway should be at least that needed for a below-average driver or vehicle to stop. According to ASSHTO's Green Book [43], sight distance is the distance allowed in roadway design for human drivers to receive information, decide on a course of action, and execute the appropriate control response. Sight distance is a design feature in roadway design and can be further broken down into stopping sight distance, decision sight distance, and passing sight distance. One of the primary factors affecting sight distance is grade. Grade is the incline or decline of a roadway as a measure of percent change from its horizontal.

Stopping sight distance is the sum of two distances: (1) the distance traversed by a vehicle from the instant the driver sights an object necessitating a stop to the instant the brakes are applied; and (2) the distance needed to stop the vehicle from the instant brake application begins. These are referred to as brake reaction distance and braking distance, respectively. In computing and measuring stopping sight distances, the height of the driver's eye is estimated to be 3.5 ft (1,080 mm) and the height of the object to be seen by the driver is 2.0 ft (600 mm), equivalent to the taillight height of the passenger car. AASHTO provides stopping sight distances on level terrain. As a general rule, the sight distance available on downgrades is larger than on upgrades, more or less automatically providing the necessary corrections for grade. Therefore, corrections for grade are usually unnecessary. An example where correction for grade might come into play for stopping sight distance would be a divided roadway with independent design profiles in extreme rolling or mountainous terrain.

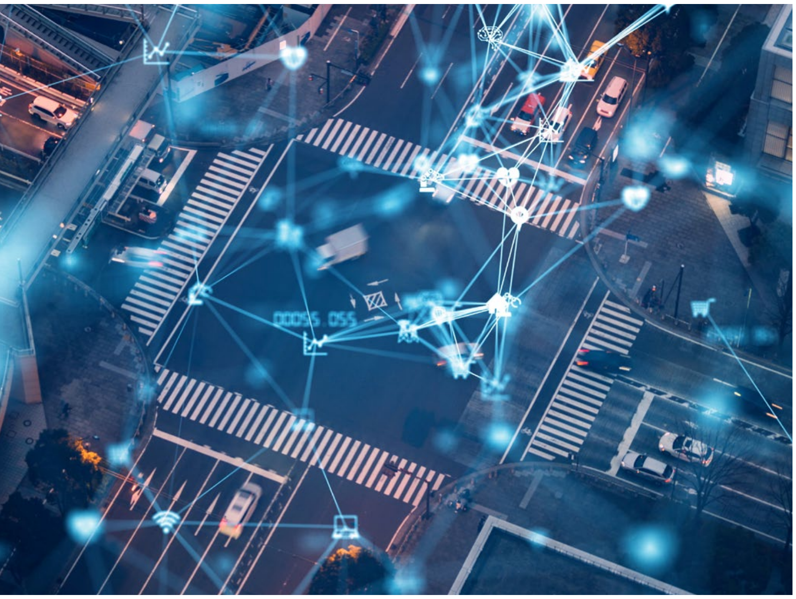
Gaps

The arrangement of geometric elements is critical for roadway design so that there is adequate sight distance for safe and efficient traffic operation. A CAV with a sensor suite under good weather conditions needs to be at least as effective as humans in obstacle detection. Vision sensors are subject to the same limitations as human sight in darkness and adverse weather conditions. While darkness is not an issue for LIDAR, this technology has thus far shown only limited success in situations with heavy rain or snow. Thus, the current technologies used on AVs do not overcome one of the major limitations with human sight – that is, line of sight. For example, at this point, it is not reasonable to assume that an AV could detect an obstacle in the roadway (such as fallen boulders) around the bend of the curve. Similarly, CAV sensors cannot see through the crest of a vertical curve. Although significant changes to roadway design standards due to differences in sight distance between human and machine are not likely based on current technology, the process of reacting/responding to a roadway obstacle once it is detected, in the form of applying the vehicle brakes, would likely be faster for the AV and could lead to modest increases in design speed, all other factors being the same (e.g., no V2X communication).

4.2.4.3 Design Elements

This subsection covers other design elements that are not related to the geometric design of a roadway and their effect on the sight distance for road users. According to the Municipality of Anchorage Project Management and Engineering Department [32], there are six design elements (plus a "general" category) that infrastructure designers use in designing an urban landscape. Common reference to these elements in ADS developers' ODD definitions can help in creating a common lexicon between ADS-operators/developers and IOOs. The six elements are:

1. **Lane –** Part of a roadway that is designated to be used by a single line of vehicles [45].



> "As roads serve different purposes, depending on their location and surrounding development, they should be designed appropriately for their function and location."

2. **Shoulder –** The portion of the roadway contiguous with the travelled way that accommodates stopped vehicles, emergency use, and lateral support of subbase, base, and surface courses [of the roadway structure] [46].
3. **Curb –** A raised or vertical element along a roadway [45].
4. **Buffer (the separation between the curb and pedestrian facilities) –** An open area that protects workers by providing motorists a place to slow down and stop if they accidentally drive through cones (or other devices) and intrude into a work zone [46]. Also referred to as a clear zone.
5. **Pedestrian facilities (e.g., sidewalks, pedestrian islands, crosswalks) –** Improvements which provide for public pedestrian foot traffic, including sidewalks, walkways, crosswalks and other improvements, such as lighting and benches which make it safe or convenient to walk [47].
6. **Landscaping –** The process of making a yard or other piece of land more attractive by altering the existing design, adding ornamental features, and planting trees and shrubs [45].

For this framework, design elements are limited to these six elements. Other elements that some consider design elements include berms, guard rails, gutters, ditches, or some support structures. These latter elements are considered as part of the geometric design of the roadway considering their significant impact on safety and determination of the relevant sight distance and curvature properties of the roadway.

Design elements are the building blocks of road composition. As roads serve different purposes, depending on their location and surrounding development, they should be designed appropriately for their function and location. Lane width has a substantial impact on the safety and comfort of the passengers in the vehicle [48]. Narrower lanes may cause CAVs to adversely react to nearby road users and may reduce capacity on a roadway [49]; however, this would also reduce vehicle speeds and create safer roadways. Wider lanes provide more desirable clearances, especially for vehicles travelling in opposite directions. Wider lanes would also necessitate fewer lanes, which would result in heavier traffic [50].

Gaps

One prominent gap that needs to be addressed is how to update standards based on safety concerns of automated vehicles. With advanced sensing and perception algorithms, the question becomes whether new roads can be designed without curbs that don't introduce incidents involving CAVs and pedestrians on sidewalks. This is especially difficult given the adversarial nature of those that may influence a CAV's performance by interfering with its connection to other devices. CAVs may also need to communicate with pedestrians on sidewalks to coordinate on their crossings at non-signalized intersections. The design of the sidewalk and its respective elements is important in determining how well a CAV can communicate with VRUs or non-road users. An area with a high density of trees or objects may limit the strength and quality of V2X messages and could limit the CAV's ability to sense objects on sidewalks or near crosswalks.

4.2.5 Architecture (Bridges, Tunnels)

CAV operation on bridges and in tunnels pose several challenges, which are discussed below.

4.2.5.1 Bridges

A bridge is a structure built to span a physical obstacle, such as a body of water, valley, or road, without closing the way underneath. It is constructed for the purpose of providing passage over the obstacle, usually something that is otherwise difficult or impossible to cross.

One of the most important CAV considerations for bridges is platoons [51]. If vehicles are able to traverse closer together, this will induce more stress on bridges from the additional weight of other vehicles traversing the bridge. Platoons may also cause greater wear on pavement and current guarding on bridges, which are not designed to withstand multiple vehicles [52]-[53]. The US alone has over 600,000 bridges (compared to 51,717 in Canada [55]) and almost four in ten bridges are 50 years or older. Of the 600,000 bridges, approximately 56,000 (~9%) of the nation's bridges were structurally deficient in 2016, and on average there were 188 million trips across structurally deficient bridges each day [54]. Platoons provide additional forces that represent a significant risk to weak bridges.

Bridges with shorter spans are likely more suited to handle platoons, considering the forces from CAV weight are divided over each pillar. Longer spans and a larger load for each pillar could cause problems for platoons. This is a primary restriction for platooning and could be expensive to alter bridges to accommodate platooning requirements. Before bridges are cleared to handle platoons, they must be upgraded to withstand higher forces, which is dependent on the size of a platoon and their respective loads.

Gaps

Regarding CAVs, strict requirements for platooning on bridges where structural loads need to account for more vehicles – many of which could have significant weights depending on the materials they're carrying – are needed to prevent premature wear or stressing of existing infrastructure.

4.2.5.2 Tunnels

A tunnel is an underground passageway, dug through the surrounding soil/earth/rock and enclosed except for an entrance and exit, commonly at each end. In the US, the National Fire Protection Agency definition of a tunnel is an underground structure with a design length greater than 23 m (75 ft) and a diameter greater than 1,800 mm (5.9 ft).

For tunnels, one of the primary considerations involves high-definition maps and lighting. Digital infrastructure and connectivity to physical infrastructure allows CAVs to maintain more accurate positioning, and this can cause lanes to be narrow along the remaining road network. This means that tunnel walls will be very close and hinder the sight distances in horizontal curves. For lower-quality tunnels, this might become an issue, and something that would require either an upgrade to the alignment or a brand-new tunnel. As both options are equally expensive, it might become problematic if this issue is a concern for many North American tunnels.

Gaps

Tunnels may require added infrastructure and connectivity options to provide accurate positioning and V2V communications for CAVs traversing through them.

4.2.6 Barriers and Work Zone Equipment

Barriers prevent and/or mitigate crashes between vehicles. They may be designed for either slower- or higher-speed traffic, depending on placement. For example, low-speed toll barrier lane crossing may consist of curbs that deter vehicles from switching lanes as they approach the toll booth, while the concrete and reinforced steel barriers typically used to separate opposing traffic on high-speed roads that lack a wide separation median are designed to prevent head-on collisions by preventing vehicles from breaching the barrier. Temporary barriers are sometimes used at work zones to protect workers from encroaching traffic.

Barriers are defined in MUTCD as any physical object that prevents access to a specific lane, or that is meant to separate distinct lanes. They keep vehicles within their roadway and prevent them from colliding with dangerous obstacles or from traversing steep (non-recoverable) slopes. Barriers can also be installed within medians of divided highways to prevent vehicles from entering the opposing roadway and help to reduce head-on collisions. Some of these barriers, designed to be struck from either side, are called median barriers. Traffic barriers can also be used to protect vulnerable areas like school yards, pedestrian zones, or work zones from vehicles entering their respective areas.

One of the primary concerns for barriers with respect to CAVs is with the CAVs' ability to sense and perceive barriers, in addition to understanding their intent. Barriers can reflect different intents, and some ADS may have trouble detecting barriers, given that the datasets they are trained on have limits on types and designs of barriers. For example, on March 23, 2018, a 2017 Tesla Model X that had the ADAS engaged had crashed into a crash attenuator at the end of a concrete median barrier. According to the performance data downloaded from the vehicle, the driver had engaged ADAS features that included traffic-aware cruise control and auto-steer lane-keeping assistance. As the Tesla approached the paved gore area dividing the main travel lanes of US-101 from the SR-85 exit ramp in Mountain View, CA, it moved to the left and entered the gore area. The Tesla continued travelling through the gore area and struck the previously damaged crash attenuator at a speed of about 71 mph (114 km/h) [55].

On the day of the crash, the crash attenuator was in a non-operational damaged state due to a previous crash, which occurred on March 12, 2018. The attenuator was not repaired before the Tesla crash on March 23 due to various factors related to scheduling and coordination among various parties that were responsible for fixing the attenuator. The National Transportation Safety Board (NTSB) investigators reviewed the crash and maintenance records and determined that the attenuator had been damaged frequently at that specific exit; in fact, it had double the repairs of any other location. As a result, one of the primary concerns for physical infrastructure in regards to CAVs is repairs. One of the recommendations from the accident report developed by NTSB suggested that MUTCD be updated to reflect time periods for repairing physical infrastructure that is damaged, as well as time periods for observing infrastructure to report damaged infrastructure appropriately [55].

Barriers tend to provide different functions and stiffness levels depending on the need, and most serve multiple functions. Examples of barrier functions include:

- To protect vehicles from roadside obstacles like bridge piers or hazards like rollover incidents;
- To prevent vehicles from crossing a median designed to separate on-coming traffic;
- To restrain a vehicle from falling off a roadway; and
- To protect workers from traffic.

Gaps

Although the design of barriers remains relatively consistent across regions compared to pavement markings and signs, one of the primary issues is in damaged or altered barriers and their intent. Because barriers serve multiple functions, it's necessary for a CAV to understand the intent of the barrier rather than simply recognizing it. Work zone barriers may indicate workers or moving equipment are nearby in which case the CAV may want to slow the driving speed significantly upon sensing a barrier. Standards that specify this type of information would facilitate safer operation of ADS-operated vehicles in work zones.

4.2.7 Accessibility

As public facilities, roadways should accommodate all users, including persons with disabilities (PWD). This section describes unique challenges for roadway infrastructure (and CAVs) in accommodating PWD.

Accessibility is defined in SAE J3171 as the degree to which a product or service is able to be accessed or used by PWD [56]. A disability is defined by the World Health Organization as an umbrella term, covering impairments, activity limitations, and participation restrictions. An impairment is a problem in body function or structure; an activity limitation is a difficulty encountered by an individual in executing a task or action; while a participation restriction is a problem experienced by an individual in involvement in life situations.

This section covers physical infrastructure components that are designed specifically for PWD. Although there is no precise terminology or definition for these components, there are several examples. For instance, an accessible crosswalk state indicator is important for individuals who suffer from hearing constraints and need to be able to clearly identify a walk sign when crossing a crosswalk at an intersection. Those with visual impairments require an audible message from the traffic signal controller that indicates when it is safe to cross. These are examples of additional infrastructure components that are put in place specifically to assist PWD in their interactions with road traffic.

In terms of accessibility, one of the key considerations for physical infrastructure and CAVs involves identifying what infrastructure may hinder a PWD from entering or exiting a vehicle. Onboarding and offboarding between a starting and ending location can be a challenging task when there are potential obstacles. CAVs need to be able to identify potential obstacles to passenger egress (e.g., light posts, mailboxes, meters, construction), and the location of accessible features (e.g., curb cutouts, ramps) around the drop-off locations and destinations in order to optimize selection of stopping locations. PWD may want to avoid specific infrastructure components like bike lanes to prevent a potential altercation with other road users. They may also want information about street lights when selecting stopping locations or the CAV to provide its own lighting of the area for safe ingress and egress.

Gaps

PWD who have cell phones may be able to utilize them to communicate with nearby infrastructure such as roadside units to receive guidance on ways they can access a CAV. Research and standards are needed to understand whether this may represent an effective solution for PWD needing to access a CAV. Additionally, infrastructure may be able to help provide updates during a route. Infrastructure can help orient an individual during their ride by providing information about their location, speed, and so on. For example, many lights can be spaced apart evenly along a road to help individuals understand how far a vehicle has gone in an urban area. Particularly for emergencies, physical infrastructure can help provide instructions on what to do if an emergency occurs. Signs can be placed to help PWD understand the best approaches for handling emergencies in CAVs.

4.3 Cybersecurity and Data Security/ Privacy

As described in the previous sections on digital and physical infrastructure, roadways make use of both, often (and increasingly) in interactive ways. While some interactive features have existed for many years (e.g., railroad crossing gates, toll booths, moveable bridges), there is a growing use of roadway digital infrastructure to enable an ever-growing list of communications-based services and functions, such as V2I and I2V-based safety and mobility applications, and the collection and transmission of vehicle trip data to support a wide range of "big data" applications. Cybersecurity and data security/ privacy risks, concerns, and mitigation strategies have flourished with the expanding use of roadway digital infrastructure to carry large volumes of very sensitive and very valuable data.

A broad definition from the United States Cybersecurity and Infrastructure Security Agency (CISA) describes cybersecurity as "the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information" [57]. This definition accounts for cybersecurity risks that are not specifically targeted to a CAV or its subcomponents. Cybersecurity that is more directly relevant to CAVs is defined in ISO 21434 (Appendix B.3) as a condition in which assets are sufficiently protected against threat scenarios to electrical or electronic components of road vehicles and their functions.

> "With the increase in types and volume of connectivity in vehicles and the increased complexity of the development of CAVs, the risks of cyberattack and the subsequent damage also increase."

Based on the CISA definition, cybersecurity not only includes protecting the electrical components of a CAV but also the networks and external devices that the CAV is connected to, either wirelessly or wired. In addition, another side of automotive cybersecurity concerns the vehicle life cycle and manufacturing principles, and data collection security. Similar to safety, cybersecurity is an emergent property and the security of the components of a CAV do not guarantee the security of the CAV as a whole.

Automotive cybersecurity covers all stages of the system engineering life cycle from design to maintenance and decommission of a CAV. In addition to electrical components, cybersecurity covers software algorithms and modules that enable CAV functionality. An important aspect has to do with protection of the connectivity and communication to external systems, such as other (CAV) vehicles, vehicle infrastructure, as well as OE vehicle manufacturer or other cloud servers. Finally, different stakeholders in the life cycle of a CAV also play an important role. The vehicle manufacturers, Tier 1 suppliers, infrastructure owners and operators, ADS developers, and additional stakeholders all share in the task of developing secure and privacy-conscious CAV systems.

With the increase in types and volume of connectivity in vehicles and the increased complexity of the development of CAVs, the risks of cyberattack and the subsequent damage also increase. CAVs will not only be more connected to external networks and devices but they will also transfer control of various subsystems within the vehicle to the human, depending on the ADS level and situation. This increasing system complexity makes it more difficult to detect cybersecurity threats, especially given "over-the-air" (OTA) connectivity and remote accessibility of systems. Initial research has uncovered a broad range of physical and remote attack surfaces that malicious agents can exploit. As vehicles continue towards ADS Level 5 implementation and increased data flows to other systems in the vehicle's environment, CAVs become further exposed to entry points for cyberattacks.

Cybersecurity and data security and privacy for CAVs is a complex field. The following is a breakdown of cybersecurity subtopics from the perspective of existing and needed standards/guidelines for a code of practice:

- Information technology and operational technology (for vehicle manufacturers)
- Cybersecurity frameworks
- Cybersecurity engineering (including security of connectivity technology and threat intelligence)
- Data privacy laws, regulations, and principles

4.3.1 Information Technology and Operational Technology

Both information technology (IT) and operational technology (OT) are necessary for supporting cybersecurity (including data security/privacy).

Traditionally, IT is defined as the use of systems (especially computers and telecommunications) for storing, retrieving, and sending information or data. OT is defined as hardware and software that monitors, manages, or controls industrial equipment, assets, processes, and events. Gradually, these two types of technologies have converged to create cyber-physical systems that not only have components controlling physical events and processes but also are integrated with hardware and software to convey and process information simultaneously.

For this document, OT controls physical processes on a manufacturing floor, or within a vehicle, including hydraulics, steering wheel, radiator, and alternator, while IT is meant to reference any system that sends or receives data (onboard or offboard).

IT and OT address different aspects of a vehicle ecosystem. As the physical and cybersecurity worlds continue to converge, the roles and responsibilities of the cybersecurity functions are evolving. One of the challenges with IT/OT integration is that these are two different cultures and supply chains; thus, the convergence is also driving cultural changes in order to address the need for greater collaboration. An example of this convergence in the standards world can be seen through the SAE and ISO cybersecurity standards.

The security monitoring infrastructure, along with credential and access validation schemes for the IT and OT, need to be flexible and scalable. The infrastructure must be able to sustain CAV deployments in the future that result in an operating performance time of a minimum of five to ten years versus the three-month application cycle upgrades for many software applications. Security infrastructure to support OT must set the foundation for the IT world to properly integrate and allow IT to scale to the appropriate levels that enable effective CAV deployments, rather than risk improper access to vehicles or their internal IT systems.

Gaps

Moreover, as the physical and cybersecurity worlds continue to converge, many challenges are encountered; notably, IT and OT are two different cultures and so the need for greater collaboration must be addressed. As partnerships continue to form between OE vehicle manufacturers and ADS developers, the culture clash is evident in the processes and standards that these types of companies participate in. From this convergence, there is a need to clearly define security responsibilities. Convergence extends even beyond the vehicle, though, as companies continue to integrate with other pre-existing infrastructure such as “smart” homes.

4.3.2 Cybersecurity Frameworks

A cybersecurity framework is a set of standards, guidelines, and best practices that an organization can follow in order to manage the cybersecurity risks it faces. Such frameworks, when adopted, help reduce a company's exposure to vulnerabilities. Risks are identified, their likelihood and impact assessed, and then they are mitigated or managed via various security measures or controls.

In the context of connected and automated vehicles, a cybersecurity framework would apply to all the ecosystem players: OE vehicle manufacturers, Tier 1 suppliers, other suppliers down the manufacturing chain, after-market integrators, software vendors, application writers, communication services providers, electric vehicle charging system entities, auto repair shops, and network or cloud services providers. It is expected that the OE vehicle manufacturers would be the party with most at stake, and so they can require evidence of adhering to certain cybersecurity framework aspects from the parties that supply them with products that are used in a vehicle. This is an ongoing process throughout the life of the CAV. For example, software and firmware updates have to be managed by the OE vehicle manufacturer in a secure fashion, as suppliers are expected to patch not just newly discovered faults but also security vulnerabilities, in a timely fashion.

While security of the in-vehicle networks has been recognized as lacking for quite some time now, the overall cybersecurity of the modern vehicle has gotten attention rapidly after the notable cyberattacks of 2014 and 2015. Now with the advent of CAVs, the attack vectors have increased dramatically. This fact, along with the recognition of supply chain complexities and the large amounts of data exchanged between CAVs and the OE vehicle manufacturer cloud and the public Internet, have resulted in a series of efforts to lay out cybersecurity frameworks applicable to the CAV ecosystem. The sources of these frameworks have been international or national standards bodies and regulatory bodies. The resulting documents, often freely available, are high level to allow for flexible implementation, and they do cover most aspects present in general cybersecurity frameworks that are clearly applicable to CAVs.

Gaps

The general and high-level nature of the cybersecurity framework leaves little room for gaps. Areas that still need attention are operational security for road infrastructure networks, which affects the trustworthiness of the V2X data communicated to the CAVs, and the resilience of the road infrastructure to attacks. In addition, there does not appear to be clear guidelines for OE vehicle manufacturers' organizational security for the driver-facing cloud services, along with a vetted approach to share CAV malware intelligence among OE vehicle manufacturers or suppliers.

4.3.3 Cybersecurity Engineering

Cybersecurity engineering refers to the art of designing systems securely from the start, incorporating measures to attain a given resilience to attacks. Cybersecurity is usually applicable to purely digital systems, but now, with the advent of intelligent "things" and especially connected and intelligent vehicles, it is applicable to cyber physical systems as well.

The scope of cybersecurity engineering for CAVs relates to the development lifecycle of the CAV, such that cybersecurity is taken into account and in harmony with safety goals. The aspects that need to be designed with cybersecurity in mind relate to electronic control unit (ECU) software and data protection, protection of in-vehicle signals and messages, separation of domains, vehicle security standards for external interfaces, and monitoring of the connected fleet of CAVs for attack prevention and resilience.

Cybersecurity engineering standardization efforts have not been as fragmented as other aspects of cybersecurity. The one international standard, ISO 21434 (Appendix B), is expected to meet that need by balancing flexibility of implementation with requirements for well-defined security controls for various aspects of the vehicle system. Complementary efforts are also currently underway with UNECE R155 requiring the operation of a certified cybersecurity management system, and UNECE R156 requiring Software Update Management Systems (SUMS). Early efforts are also underway at SAE to develop additional technical requirements documentation building off of UNECE 155/156.

Gaps

With the risk of reducing the opportunity for innovation and evolution, there may still be a need for best practices for *modern* in-vehicle platform architecture protection, from sensors to ECUs to gateways. For example, Ethernet-based architecture with few gateways each acting as gatekeepers for a network of less-capable ECUs and other components communicating via insecure buses can handle cross-domain communication in a potentially more secure manner. It is possible that these principles are planned to be addressed in the Adaptive AUTOSAR platform standardization effort.

4.3.3.1 Cybersecurity of Connectivity Technology

An important aspect of cybersecurity engineering relates to communications between CAVs and other entities in the system (other CAVs, road infrastructure, OE vehicle manufacturer cloud servers). Connectivity technology allows for message passing between entities that don't necessarily trust each other from the beginning, and thus it requires careful specification and implementation. For the purposes of this study, connectivity technology (CT) refers to technologies that enable the operation of connectivity features that transfer and/or receive data and are installed in vehicles by their manufacturer. Examples are Wi-Fi, broadband cellular, Bluetooth, and V2X communications. This definition of CTs only includes technologies that enable the transfer of data on to and off the vehicle and excludes technologies that enable inter-subsystem communication within a vehicle, such as the controller area network (CAN) bus.

Wireless connectivity technologies are those that utilize a radio frequency (RF) transmitter, receiver, or transceiver in order to facilitate wireless communications. Most modern vehicles now contain an onboard cellular modem providing this broadband connectivity, or they can be connected to the cellular networks via a handheld mobile device plugged into the vehicle. Two other common types of communication technologies components on a modern vehicle are the Wi-Fi transceiver, which provides offboard Wi-Fi connectivity, and the Bluetooth, which allows connecting to nearby or on-vehicle devices. Lastly, Cellular V2X (C-V2X) is a short-range radio technology that allows messages to be exchanged among neighbouring vehicles or between vehicles and road infrastructure.

External connectivity technologies are an integral function of CAVs, which is well-defined and mature, with known threats and mitigations, as they have been used in other ecosystems before they were adopted (or planned) into CAVs. New vulnerabilities may be discovered over time. Of all these communications technologies, V2X communications are the only ones specific to vehicles, but this technology has been around for more than a decade, with protocol-level and security infrastructure security measures well specified and subject to public scrutiny. Further, recent security controls for the entire V2X communication system, including onboard units and road-side unit security devices, are in the process of being addressed.

Gaps

One of the largest gaps in connectivity cybersecurity technology is the lack of clear and uniform SCMS definitions of misbehaviour. As an SCMS is used for misbehaviour detection and reporting, it is important to have a well-defined understanding of the range of severity as it relates to misbehaviour and the required response from the system.

4.3.3.2 Misbehaviour Detection for V2X Communications

Misbehaviour is a type of incorrect functioning by a participant of a network of connected nodes. It has been applied to vehicular networks, be it within a vehicle network of ECUs, or in a cooperative driving automation system involving vehicles and infrastructure communicating with each other. It involves detection, reporting, and removal of untrustworthy actors.

Misbehaviour detection is generally assumed to apply to vehicular networks, where end nodes exchange messages. Thus, for the CAV networks, which are expected to enjoy an even richer set of communication technologies and to exchange even more data, misbehaviour detection becomes paramount. The US Department of Transportation has begun a National SCMS Development project to explore potential approaches for the establishment and governance of a National SCMS used for misbehaviour detection and reporting. The goal of the National SCMS Development project is to develop a National SCMS Deployment Strategy to help the Department of Transportation and industry establish a viable National SCMS ecosystem in support of V2X communications [60].

In this context, a CAV sends V2X messages in support of a given application to other CAVs or road infrastructure (e.g., RSU). The aspects of misbehaviour encompass procedures applied to both the CAV and the V2X network:

- CAV procedures: Misbehaviour detected in the received V2X messages, followed by reporting to a central server such as a misbehaviour authority (MA). Reporting may not be undertaken if the message is clearly incorrect and can be discarded locally. Reporting is expected for unclear cases where a central authority can make a more informed decision from inputs from many reports received.
- Network MA procedures: Gathering misbehaviour reports and determining whether a reported CAV is no longer trustworthy, followed by removal of such CAV from participating in that V2X application by publishing its identifiers in a certificate revocation list (CRL). CRLs are downloaded by CAVs periodically

to aid in checking received V2X message for trustworthiness of the sender. Note: IEEE 1609.2.1 (Appendix B.1) describes a mechanism where all certificates are loaded into the vehicles in advance but are locked and cannot be used without an "unlock" key. This mechanism could be used for lower priority misbehaviour actions as a means of improving overall SCMS ecosystem health.

Misbehaviour in V2X communications is a liability-sensitive matter for OE vehicle manufacturers, and hence the standards evaluated are limited to threat analyses for V2X communication and a foundational misbehaviour detection for V2X messages. Misbehaviour detection and reporting for V2X messaging is currently under development in various standards development organizations (SDOs) and industry forums and has to be done for each V2X application separately. V2X messaging is crucial for cooperative driving and is the avenue that connects vehicles from different manufacturers with each other and with the road infrastructure. Hence cooperation and standardization is required to achieve the goal of timely removal of corrupted vehicles from participating in this type of communication system.

Gaps

Similar to the previous section that broadly describes gaps in connectivity technology, one of the largest gaps regarding SCMS is the current lack of a clear definition for misbehaviour.

4.3.3.3 Threat Intelligence

In order to effectively manage cyber and privacy risks, it is necessary to understand the specific threats that exist, given the type and extent of the digital network being protected. The National Institute of Standards and Technology (NIST) defines "threat intelligence" as "threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes" [61]. The NIST SP 800-150, "Guide to Cyber-Threat Information Sharing" [62] is generally applicable to cyber systems, including cyber-physical systems. In the context of CAVs, threat intelligence relates to the operation of collecting threats to any component of a CAV or to the external systems it interacts with, analyzing such threats, and assessing measures to protect all systems that could be affected by them.

The automotive world has traditionally seen little collaboration among OE vehicle manufacturers. Fierce competition and the need for intellectual property protection (along with the liability sensitivity already mentioned) have discouraged collaboration in terms of lessons learned. This challenge is now being overcome by the need to share threat intelligence because of the increased attacks on the CAVs and the networks that they connect to. The architecture of vehicle networks, with highly specialized ECUs and obscured architectures, have slowed down the malware evolution, compared to, say, smartphone platforms, which are rather few and open. However, with the evolution towards more generic ECUs with software-driven customization, malware threats may become more "contagious". The standards evaluated are limited to a high level of integrity classifications, summary of threat intelligence principles from an OE vehicle manufacturer forum. For example, open protocols such as J1939 and J1979 pose (Appendix B.3) potential risks for spoofing and data misrepresentation through integrated fleet management systems and external parties that may be able to access systems remotely.

Gaps

Given that threat intelligence is something that OE vehicle manufacturers may wish to keep close to themselves and only share data that are of mutual benefit to them and others, it is difficult to assess whether there are gaps in the threat intelligence community applicable to CAVs. Threat intelligence in the US is being addressed by the automotive industry via the Automotive Information Sharing and Analysis Center (Auto-ISAC) [58] whose mission is to keep in step with the development of malware at an industry level. As such, there are no specific gaps to report for this section.

"Concern over data privacy has grown along with the trend of increasing data capture and use."

4.3.4 Data Privacy Laws, Regulations, and Principles

Data privacy encompasses the aspects of collection of information and its dissemination. Due to the public's general expectation of privacy of data, there exist legal and political issues relating to data privacy. Concern over data privacy has grown along with the trend of increasing data capture and use. While privacy protection was initially more concerned with government violation of citizens' privacy "rights", the concern has shifted more towards the violation of consumers' privacy by big businesses. In addition to mitigating the risk of identity theft, consumer advocates have pursued the "right to be forgotten" in Internet searches and proposed a range legal limits on private surveillance techniques.

In the context of the global auto industry, privacy laws and regulations are generally treated as a pool of requirements, the most stringent set of which become the de facto global privacy requirements. This is effectively necessitated by the need for data security and privacy protection to be designed into the vehicle architecture as well as into all subsequent data handling practices throughout the entire vehicle life cycle. This makes the management of *market-level* security and privacy requirements through variable product designs impracticable from a global business standpoint for such a complex product.

Currently, the two most stringent privacy requirements affecting motor vehicles are the European Union (EU) General Data Protection Regulation (GDPR) and the California Consumer Privacy Protection Act (CCPA), as most recently modified by the California Privacy Rights Act (CPRA) passed by referendum in November 2020.

Gaps

None identified.

5. Conclusions

The development of a code to address the specific needs of CAVs with regard to physical and digital infrastructure and appropriate cybersecurity overhead would support and promote their further deployment in North America to the benefit of the travelling public, as well as those charged with implementing and maintaining roadway infrastructure. This framework describes the current state of the art with respect to the physical and digital infrastructure and cybersecurity overhead for human-operated vehicles and identifies gaps regarding standards and specifications for vehicles equipped with connectivity and driving automation technologies, including those capable of driverless operation.

Digital infrastructure that is interoperable (i.e., standardized for all connected traffic participants), as well as connected to a backhaul network with Internet/ cloud connectivity, is needed in order to provide the full range of anticipated benefits from CAVs. These include cooperative driving automation features that enable safer and/or more efficient outcomes than can be provided by CAVs operating independently of one another. Finally, HD maps, which are essential to the safe operation of CAVs, require timely and accurate data about changes to road/weather infrastructure (e.g., work zones, weather events, evacuation).

Some of the salient gaps related to digital infrastructure include:

- Lack of specifications for digital infrastructure governance and edge/cloud computing needs and means.
- The SCMS lacks a formal and legally sanctioned governance framework and authority, which it requires in order to issue and enforce SCMS rules of operation (especially important for cross-border operations).
- First responder guidance for ADS-dedicated vehicles.
- GPS accuracy enhancement and base stations for differential correction.
- Support for HD mapping of temporary traffic zones (e.g., work zones, incident scenes).

Physical infrastructure that is consistent across internal jurisdictional boundaries and well maintained can both greatly improve the reliability of CAVs and substantially increase their range (i.e., operational design domain). Consistent standards – especially for markings, signage, and signals – would not only facilitate the deployment of driving automation technologies but would support improved performance by human drivers (with and without ADAS features). Care, however, should be taken not to tailor standards too closely to current sensing technologies to the extent possible, so as not to inadvertently constrain the development of new and improved sensing and communications technologies.

Some of the salient gaps related to physical infrastructure are identified here:

- There is a lack of infrastructure standards and test procedures for vehicle-to-infrastructure communication. There are standards for specific message types and how they can be communicated, but there is a gap in understanding how data can be fused at an intersection so that perception data from various sources can be amalgamated to help prevent crashes.
- Standards are also needed to address data quality, response times, and responsibilities during exchanges (i.e., handshakes).
- There is a need to understand how different types of crosswalk markings affect CAVs. Sensing and perception algorithms must be able to appropriately detect and react to different crosswalk markings without confusing them for other types of road surface markings, such as lane markings, fire lane guidance warnings, or warnings not to enter a specific road surface area. In addition, novel crosswalk designs that are not relevant to crosswalk safety also pose problems for CAVs.
- With regard to intersections, there is a gap in understanding how data can be fused at an intersection so that perception data from various sources can be amalgamated to help prevent crashes.
- Bridges need to be evaluated for their ability to safely handle close-coupled platoons of vehicles – especially loaded trucks. It is important to ensure that bridges can safely bear the weight without suffering damage.
- Long tunnels may require additional digital infrastructure to facilitate V2V communications, as well as to augment GPS location data.

Maintaining adequate cybersecurity and data privacy for CAVs is essential to gaining and maintaining the public's trust in wider CAV deployment. There are several communications technologies that CAVs can use to exchange data with each other and with infrastructure, and each comes with privacy and security challenges. While cybersecurity is tailored to each organization and its specific needs based on technology and design, there are well-established security frameworks and engineering practices that can improve a system-wide security posture. There is a need in particular for guidance tailored to help public sector agencies assess and mitigate cybersecurity risks with limited resources. Privacy is governed by legal and regulatory frameworks at the international,

national, and local levels. In North America, it is addressed by industry or by technology, rather than as a common property of connected living things (i.e., the Internet of Things).

In general, cybersecurity is rather intolerant of gaps, but there are a few areas that could benefit from standardization:

- Standards defining operational security for road infrastructure networks are needed to establish the trustworthiness of the V2X data communicated to the CAVs, along with the resilience of the road infrastructure to withstand cyberattacks.
- Guidelines are needed for vehicle manufacturers' organizational security for the driver-facing cloud services, along with a vetted approach to share CAV malware intelligence among OE vehicle manufacturers and with their suppliers.
- As manufacturers migrate to more modern electronic/electrical (E/E) architectures, such as Ethernet-based architectures, there is a growing need for standards to address unique security challenges.

A code that addresses these specific areas within the digital and physical infrastructure topic areas would significantly improve the safety and security of CAV implementation within North America. The National Highway Traffic Safety Administration (NHTSA) released the Automated Vehicles Comprehensive Plan in January 2021 [63], which defines one of the major objectives of the administration: to "update infrastructure standards to reflect ADS technologies". Addressing these findings in a code of practice would accelerate the national vision of ADS-relevant infrastructure in North America and satisfy a key enabler for CAV deployments across the continent.

References

[1] G. Knapp, M. Bullock, and C. Stogios, "Connected and Automated Vehicle Technologies – Insights for Codes and Standards in Canada," June 2020. [Online]. Available: https://www.csagroup.org/article/research/connected-and-automated-vehicle-technologies-insights-for-codes-and-standards-in-canada/

[2] Government of Canada, "Projects Funded by the Program to Advance Connectivity and Automation in the Transportation System," May 7, 2019. [Online]. Available: https://tc.canada.ca/en/road-transportation/innovative-technologies/automated-connected-vehicles/projects-funded-program-advance-connectivity-automation-transportation-system

[3] Infrastructure Canada, "Smart Cities Challenge Map of Applicants," Government of Canada. [Online]. Available: https://www.infrastructure.gc.ca/sc-vi/map-applications.php (accessed Mar. 1, 2021).

[4] U.S. Department of Transportation, "Fixing America's Surface Transportation Act," Federal Highway Administration. [Online]. Available: https://www.fhwa.dot.gov/fastact/ (accessed Dec. 20, 2020).

[5] Transportation Research Board, "NCHRP 20-102(15), Impacts of Connected and Automated Vehicle Technologies on the Highway Infrastructure," The National Academies of Sciences, Engineering, and Medicine, May 24, 2018. [Online]. Available: https://apps.trb.org/cmsfeed/TRBNetProjectDisplay.asp?ProjectID=4377

[6] Transportation Research Board, "NCHRP 20-102(24), Infrastructure Modifications to Improve the Operational Domain of Automated Vehicles," The National Academies of Sciences, Engineering, and Medicine. [Online]. Available: https://apps.trb.org/cmsfeed/TRBNetProjectDisplay.asp?ProjectID=4680 (accessed Dec. 20, 2020).

[7] Transportation Association of Canada, *Manual of Uniform Traffic Control Devices for Canada,* 5th ed., 2014. [Online]. Available: https://www.tac-atc.ca/en/5th-edition-manual-uniform-traffic-control-devices-canada

[8] U.S. Federal Highway Administration, *Manual on Uniform Traffic Control Devices,* 2009. [Online]. Available: https://mutcd.fhwa.dot.gov/htm/2009/part1/part1a.htm#section1A13

[9] U.S. Department of Transportation, *Status of the Nation's Highways, Bridges, and Transit: Conditions & Performance,* Dec. 16, 2016. [Online]. Available: https://www.fhwa.dot.gov/policy/2015cpr/pdfs/2015cpr.pdf

[10] British Standards Institute, "CAV Roadmap," 2020. [Online]. Available: https://www.bsigroup.com/en-GB/CAV/cav-resources/download-cav-roadmap/

[11] BSI Standards Development, "PD ISO/TR 4609 – Road Vehicles – Report on Standardization Prospective for Automated Vehicles (RoSPAV)" [Online]. Available: https://standardsdevelopment.bsigroup.com/projects/2019-03903#/section (accessed Aug. 19, 2021).

[12] Public Safety Canada, "National Strategy for Critical Infrastructure," Government of Canada, 2009. [Online]. Available: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf

[13] G,A, Golembiewski and B Chandler, "Intersection Safety: A Manual for Local Rural Road Owners," U.S. Federal Highway Administration, Jan. 2011. [Online]. Available: https://safety.fhwa.dot.gov/local_rural/training/fhwasa1108/fhwasa1108.pdf

[14] Alberta Transportation, "Intersections," Government of Alberta, Feb. 5, 2021. [Online]. Available: https://www.alberta.ca/intersections.aspx

[15] E-H Chou, "Crash Factors in Intersection-Related Crashes: An On-Scene Perspective," U.S. National Highway Traffic Safety Administration, Sept. 2010. [Online]. Available: https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/811366

[16] F. Chen, M. Song, and X. Ma, "Investigation on the Injury Severity of Drivers in Rear-End Collisions between Cars Using a Random Parameters Bivariate Ordered Probit Model," *Int. J. Environ. Res. Public Health,* vol. 16, pp. 26-32, 2019.

[17] T-Y. Liao and R. Machemehl, "Fuel Consumption Estimation and Optimal Traffic Signal Timing," Southwest Region University Transportation Center, University of Texas, Aug. 1998. [Online]. Available: https://static.tti.tamu.edu/swutc.tamu.edu/publications/technicalreports/467312-1.pdf

[18] C. Hendrickson, A. Biehler, and Y. Mashayekh, "Connected and Autonomous Vehicles 2040 Vision," Pennsylvania Department of Transportation, Jul. 10, 2014. [Online]. Available: https://traffic21.heinz.cmu.edu/wp-content/uploads/sites/23/2020/02/Joint-Statewide-Connected-and-Autonomous-Vehicles-2040-Vision-Final-Report-smaller.pdf

[19] U.S. Department of Transportation, "Eco Approach and Departure at Signalized Intersection," 2013. [Online]. Available: https://www.fhwa.dot.gov/publications/research/operations/15011/15011.pdf

[20] *Intelligent Transport Systems – Cooperative ITS – Using V2I and I2V Communications for Applications Related to Signalized Intersections*, ISO 19091, 2017. [Online]. Available: https://www.iso.org/standard/69897.html

[21] C. V. Zeeger *et al.,* "Safety Effects of Marked Versus Unmarked Crosswalks at Uncontrolled Locations: Final Report and Recommended Guidelines," U.S. Federal Highway Administration, Aug. 2005. [Online]. Available: https://www.fhwa.dot.gov/publications/research/safety/04100/04100.pdf

[22] Government of British Columbia, *Motor Vehicle Act,* Chapter 318, Part 3, 10 Mar. 2021. [Online]. Available: https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96318_05

[23] M. Sucha, D. Dostal, and R. Risser, "Pedestrian-Driver Communication and Decision Strategies at Marked Crossing," *Accid. Anal. Prev.,* vol. 102, pp. 41–50, 2017, doi: 10.1016/j.aap.2017.02.018.

[24] A. Rasouli and J. Tsotsos, "Autonomous Vehicles that Interact with Pedestrians: A Survey of Theory and Practice," *IEEE Trans. Intell. Transp. Syst.,* vol. 21, no. 3, pp. 900–918, Mar.2020, doi: 10.1109/TITS.2019.2901817.

[25] N. Gueguen, S. Meineri, and C. Eyssartier, "A Pedestrian's Stare and Drivers' Stopping Behavior: A Field Experiment at the Pedestrian Crossing," *Saf. Sci.,* no. 75, pp. 87-89, 2015.

[26] N. Merat *et al.,* "What Externally Presented Information Do VRUs Require When Interacting with Fully Automated Road Transport Systems in Shared Space?" *Accid. Anal. Prev.,* vol. 118, pp. 244–252, Sept. 2018, https://doi.org/10.1016/j.aap.2018.03.018.

[27] K. Saleh, M. Hossny, and S. Nahavandi, "Towards Trusted Autonomous Vehicles from Vulnerable Road Users Perspective," 2017 *IEEE International Systems Conference (SysCon),* 2017, pp. 1–7, doi: 10.1109/SYSCON.2017.7934782.

[28] D. Shinkle, "Pedestrian Crossing: 50 State Summary," *Proceedings of National Conference of State Legislatures,* Washington, DC, USA, 2016.

[29] S. Jayaraman, *et al.,* "Pedestrian Trust in Automated Vehicles: Role of Traffic Signal and AV Driving Behavior," *Front. Robot. AI,* 28 Nov. 2019, https://doi.org/10.3389/frobt.2019.00117.

[30] Teague, "Crossing the Road in the World of Autonomous Cars." [Online]. Available: https://teague.com/insights/labs/crossing-the-road-with-autonomous-cars (accessed Aug. 27, 2021).

[31] A. Rasouli, K. Kotseruba, and J. Tsotsos, "Agreeing to Cross: How Drivers and Pedestrians Communicate?" *2017 IEEE Intelligent Vehicles Symposium (IV),* pp. 264–269, Jun. 2017, doi: 10.1109/IVS.2017.7995730.

[32] M. McFarland, "Elon Musk Vents about California's Lane Markings Confusing Tesla's Autopilot," *The Washington Post*, 2015. https://www.washingtonpost.com/news/innovations/wp/2015/10/14/elon-musk-vents-about-californias-lane-markings-confusing-teslas-autopilot/. (accessed Oct. 14, 2015).

[33] A. Sage, "Where's the Lane? Self-Driving Cars Confused by Shabby U.S. Roadways," Reuters, Mar. 31, 2016 https://www.reuters.com/article/us-autos-autonomous-infrastructure-insig/wheres-the-lane-self-driving-cars-confused-by-shabby-u-s-roadways-idUKKCN0WX131

[34] European Road Assessment Program (EuroRAP) and Euro NCAP, "Roads That Cars Can Read: A Quality Standard for Road Markings and Traffic Signs on Major Rural Roads: Proposals for Consultation," Nov. 2013. [Online]. Available: https://www.eurorap.org/wp-content/uploads/2015/03/roads_that_cars_can_read_2_spread1.pdf

[35] Q. Guo, L. Li, and X. Ban, "Urban Traffic Signal Control with Connected and Automated Vehicles: A Survey," *Transp. Res. Part C Emerg. Technol.,* vol. 101, pp. 313–334, Aprl. 2019, https://doi.org/10.1016/j.trc.2019.01.026.

[36] H. Aziz *et al.,* "Synthesis Study on Transitions in Signal Infrastructure and Control Algorithms for Connected and Automated Transportation," Oak Ridge National Laboratory, Jun. 20, 2017. [Online]. Available: https://info.ornl.gov/sites/publications/files/Pub75211.pdf

[37] U.S. Federal Highway Administration, "A5: Employ Emergency Vehicle Preemption," Signalized Intersection Safety Strategies, 2013. [Online]. Available: https://safety.fhwa.dot.gov/intersection/other_topics/fhwasa08008/sa5_emergency_vehicle.pdf

[38] Transportation Systems Management and Operations, "Freight or Truck Signal Priority," Washington Department of Transportation. [Online]. Available: https://tsmowa.org/category/signal-operations/freight-or-truck-signal-priority (accessed Aug. 27, 2021).

[39] Alberta Government, "Wildlife Crossing Signs," Nov. 2015. [Online]. Available: http://www.transportation.alberta.ca/Content/docType233/Production/65Wildlife_Crossing_signs.pdf

[40] Pierce County, Washington Local Authority, "Mount Rainier Active Volcano." [Online]. Available: https://www.piercecountywa.org/3730/Mount-Rainier-Active-Volcano (accessed Aug. 27, 2021).

[41] CAA Quebec, "Photo Radar and Red-Light Cameras." [Online]. Available: https://www.caaquebec.com/en/on-the-road/public-interest/road-safety/photo-radar-and-red-light-cameras/ (accessed Aug. 27, 2021).

[42] TECH Policy Lab at the University of Washington, "New Research on Adversarial Machine Learning," Oct. 16, 2018. [Online]. Available: https://techpolicylab.uw.edu/news/new-research-on-adversarial-machine-learning/

[43] American Association of State Highway and Transportation Officials, *A Policy on Geometric Design of Highways and Streets,* 7th ed. Washington, DC, USA: AASHTO, 2018.

[44] J. Khoury, K. Amine, and R. Saad, "An Initial Investigation of the Effects of a Fully Automated Vehicle Fleet on Geometric Design," *J. Adv. Transp.,* vol. 2019, Article ID 612640, https://doi.org/10.1155/2019/6126408.

[45] Merriam-Webster.com, "lane," https://www.merriam-webster.com/dictionary/lane; "curb," https://www.merriam-webster.com/dictionary/curb; "landscaping," https://www.merriam-webster.com/dictionary/landscaping (accessed Aug. 27, 2021).

[46] Cambridge University Dictionary.com, "shoulder," https://www.dictionary.com/browse/shoulder; "buffer," https://www.dictionary.com/browse/buffer (accessed Aug. 27, 2021).

[47] Washington State Department of Transportation, "Pedestrian Facilities Guidebook," Sept. 1997. [Online]. Available: https://safety.fhwa.dot.gov/saferjourney1/library/pdf/pedfacguide.pdf

[48] T. Petritsch, "The Influence of Lane Widths on Safety and Capacity: A Summary of the Latest Findings," Sprinkle Consulting. [Online]. Available: https://nacto.org/docs/usdg/lane_widths_on_safety_and_capacity_petritsch.pdf (accessed Aug. 27, 2021).

[49] I. Potts, D. Harwood, and K. Richard, "Relationship of Lane Width to Safety for Urban and Suburban Arterials," *J.Transport. Res. Rec.,* pp. 63–82, Dec. 2007, https://doi.org/10.3141/2023-08.

[50] W. S. Homburger *et al., Fundamentals of Traffic Engineering,* 14th ed. Berkeley, CA, USA: University of California – Berkeley, 1996.

[51] Y. Hayeri, C. Hendrickson, and A. Biehler, "Potential Impacts of Vehicle Automation on Design, Infrastructure and Investment Decisions – A State DOT Perspective," presented at the Transportation Research Board 9th Annual Meeting, Washington DC, USA, Jan. 11–15, 2015.

[52] O. Carsten and R. Kulmala, "Road Transport Automation as a Societal Change Agent," presented at the Transportation Research Board 9th Annual Meeting, Washington, DC, USA, Jan. 11–15, 2015.

[53] F. Chen, R. Balieu, and N. Kringos, "Potential influences on Long-Term Service Performance of Road Infrastructure by Automated Vehicles," *J. Transport. Res. Rec.,* vol. 2550, pp. 72–79, 2016.

[54] American Society of Civil Engineers, "2017 Infrastructure Report Card," 27 May 2017. [Online]. Available: https://www.infrastructurereportcard.org/wp-content/uploads/2016/10/2017-Infrastructure-Report-Card.pdf

[55] U.S. National Transportation Safety Board, "Crash Summary Report of Highway Investigation HWY18FH011 Involving a Tesla Model X," Feb. 2018. [Online]. Available: https://data.ntsb.gov/Docket?NTSBNumber=HWY18FH011

[56] *Identifying Automated Driving Systems-Dedicated Vehicles (ADS-DVs) Passenger Issues for Persons with Disabilities,* SAE J3171, SAE International, Washington DC, USA, 2019.

[57] Cybersecurity and Infrastructure Security Agency, "Security Tip (ST04-001): What Is Cybersecurity?" Nov. 14, 2019. [Online]. Available: https://us-cert.cisa.gov/ncas/tips/ST04-001

[58] Auto-ISAC, "Automotive Information Sharing and Analysis Center." [Online]. Available: https://automotiveisac.com/ (accessed Apr. 26, 2021).

[59] G. Vlieg, "Canadian Model Rules of the Road", PTM-RULES18-E, Transportation Association of Canada, 2018. Available: https://www.tac-atc.ca/sites/default/files/site/doc/Bookstore/english_for_publishing.pdf

[60] United States Department of Transportation, “Security Credential Management System (SCMS).” [Online]. Available: https://www.its.dot.gov/resources/scms.htm (accessed Aug. 25, 2021).

[61] Information Technology Laboratory, “Cyber-Threat Intelligence and Information Sharing,” ITL Bulletin for May 2017. [Online]. Available: https://csrc.nist.gov/csrc/media/publications/shared/documents/itl-bulletin/itlbul2017-05.pdf

[62] C. Johnson *et al.,* “Guide to Cyber-Threat Information Sharing,” National Institute of Standards and Technology, Oct. 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

[63] U.S. Department of Transportation, "Automated Vehicles Comprehensive Plan," The National Highway Traffic Safety Administration [Online]. Available: https://www.transportation.gov/sites/dot.gov/files/2021-01/USDOT_AVCP.pdf (accessed Jan. 11, 2021).

Appendix A – Sample Expert Interview Questions

A.1 Digital Infrastructure

- Are the current digital infrastructure standards uniformly applicable across the North American market, including Canada, the United States, and Mexico?
- Do current DSRC standards sufficiently address spectrum, hardware, and latency requirements for current and future connected and autonomous vehicle applications?
- What gaps are you aware of that currently exist with respect to CAV digital infrastructure-relevant standards?
- Without an established standard of data quality, how is interoperability of maps from different providers ascertained?
- Would map production or usage benefit from having a standardized way to evaluate a map or mapping process, or a standardized measure of quality for map data?
- Are you aware of any conflicts between SAE J2735, ISO 15628:2013, ISO 18750:2018, or ISO 17572-1:2015 as it relates to enabling vehicle automation and shared data?
- Do you see any opportunities for further enhancement to the existing standards related to enabling automation and integrating shared maps?
- There are currently no AV Fleet management standards in place. Do you foresee this as a future need for your organization, if so why?
- Do current standards sufficiently address the needs of both commercial and personal vehicle Autonomous Vehicle development and deployment?
- Do existing standards sufficiently address the range of topology, regulation, and infrastructure development variation observed across the entire North American market?
- Are existing digital infrastructure standards developing at a pace suitable to address the rapid improvements in both hardware and software associated with connected and autonomous vehicles?

A.2 Sample Physical Infrastructure

- Does MUTCD provide a level of specification necessary to develop a standard?
- Does the MUTCD provide sufficient guidance for CAV deployment in North America?
- Do the revisions to MUTCD involving ADS have gaps related to Cooperative Driving Automation?
- Does AASHTO roadside design guide conflict with the MUTCD or NTCIP 1203?
- Are there discrepancies between CA MUTCD and FHWA MUTCD? If so, can you describe them?
- What gaps currently exist with respect to CAV physical infrastructure-relevant standards?

- Do Canadian provincial or local standards differ from US state or local standards? How so?
- Are there standards not in SAE or ISO that should be included in a North American CAV Framework involving physical infrastructure? (IEEE, UNECE, ASAM, etc.)?
- What physical infrastructure is different currently between the US and Canada (traffic signals colors/timing, lane markings, signs, etc.)?
- Do standards involving work zones have guidance for ADS such as types of messages that need to be sent from infrastructure to the ADS-DV?
- Do standards with maintenance requirements need to be regularly updated to account for ADS sensor suites involving cameras, LIDAR, radar, etc.?

A.3 Sample Cybersecurity

- What are the first standards expected to provide specifications or requirements rather than guidelines for cybersecurity?
- Do any of the 8 principles in PAS 1885 conflict with the principles defined in ISO 4804?
- Does the ISO 4804 methodology account for CAV deployment?
- What differences exist between Canadian and North American cybersecurity standards?
- Does the UNECE Cybersecurity and OTA Software standard or the General Data Protection Regulation present conflicts for the SAE or ISO standards on cybersecurity? If so, what are the implications since Japan and Korea both have adopted this regulation for SAE Level 3 vehicles?
- What proposals are in place to work on future cybersecurity standards in ISO? How do the proposals build from the technical requirements and methodologies being put into place in current documents?
- Does the California Consumer Privacy Act conflict with guidance set forth by NHTSA in the Best Practices for Cybersecurity in Modern Vehicles?
- Do current standards or guidelines address adversarial attacks on CAVs (phishing, hacking, Denial of Service, etc.)?

Appendix B – Relevant Standards, Publications, and Activities

B.1 Digital Infrastructure

Alberta Transportation Driver's Guide to Operation, Safety and Licensing: Cars and Light Trucks

ASAM OpenODD

ASTM F3200:20a: Standard Terminology for Driverless Automatic Guided Industrial Vehicles

British Columbia Motor Vehicle Act

Canadian Highway Bridge Design Code

CEN/TS 17395:2020 – Intelligent Transportation Systems – eSafety – eCall for Automated and Autonomous Vehicles

CEN 17240:2018 – Intelligent Transportation Systems – eSafety – eCall End to End Conformance Testing for IMS Packet Switched Based Systems

CEN 17182 – Intelligent Transportation Systems – eSafety – eCall via an ITS-station

CEN EN16072 – Intelligent Transportation Systems – eSafety – Pan-European eCall Operating Requirements

CEN EN16102 – Intelligent Transportation Systems – eCall – Operating Requirements for Third Party Support

DFT TRO Candidate Common Data Models and Policy Review 2019

ETSI TS 102 486-x – Intelligent Transportation Systems – Road Traffic Telematics

ETSI 302 895 – Intelligent Transportation Systems – Vehicular Communications

ETSI TR 102 863 – Intelligent Transportation Systems – Local Dynamic Map (LDM)

ETSI EN 302 637-2 – Intelligent Transportation Systems – Specification of Cooperative Awareness Basic Service

ETSI TS 101 539-1 – Intelligent Transportation Systems – Road Hazard Signaling (RHS)

ETSI TR 103 300-1 – Intelligent Transportation Systems – Use Cases Definition

IEEE 802.11 – Medium Access Control (MAC) and Physical Layer (PHY) for Wireless Local Area Networks (WLAN)

IEEE 1609 – Wireless Access in Vehicular Environments (WAVE)

ISO 14296 – Intelligent Transportation Systems – Extension of Map Database Specifications for Applications of Cooperative ITS

ISO 14825 – Intelligent Transportation Systems – Geographic Data Files (GDF)

ISO 15628 – Intelligent Transport Systems – Dedicated Short Range Communication (DSRC) – DSRC Application Layer

ISO 16845-x:2016 – Road Vehicles – Controller Area Network (CAN) Conformance Test Plan – Part 1: Data Link Layer and Physical Signalling

ISO 11898-x:2015 – Road Vehicles – Controller Area Network (CAN) – Part 1: Data Link Layer and Physical Signalling

ISO 15765-x:2011 – Road Vehicles – Diagnostic Communication over Controller Area Network (DoCAN) – Part 4: Requirements for Emissions-related Systems

ISO 17572 – Intelligent Transport Systems (ITS) – Location Referencing for Geographic Databases – Part 1: General Requirements and Conceptual Model

ISO 18750 – Intelligent Transport Systems – Co-operative ITS – Local Dynamic Map

ISO 19116:2019 – Geographic Information – Positioning Services

ISO 22951 – Data Dictionary and Message Sets for Preemption and Prioritization Signal Systems for Emergency and Public Transport Vehicles (PRESTO)

ISO 26262-9:2019 – Road Vehicles – Functional Safety – Part 9: Automotive Safety Integrity Level (ASIL)-Oriented and Safety-Oriented Analyses

ISO NP 23150 – Road Vehicles – Data Communication between Sensors and Data Fusion Unit for Automated Driving Functions – Logical Interface

ISO/TS 17424 – Intelligent Transport Systems – Cooperative Systems – State of the Art of Local Dynamic Maps Concepts

ISO/TS 19321 – Intelligent Transport Systems – Cooperative ITS – Dictionary of In-Vehicle Information (IVI) Data Structures

ISO/TS 21184 – Cooperative Intelligent Transport Systems (C-ITS) – Global Transport Data Management (GTDM) Framework

ISO/TS 21219-19:2016 – Intelligent Transport Systems – Traffic and Travel Information (TTI) via Transport Protocol Experts Group, Generation 2 (TPEG2) – Part 19: Weather Information (TPEG2-WEA)

ISO/TR 21718:2019 – Intelligent Transport Systems – Spatio-Temporal Data Dictionary for Cooperative ITS and Automated Driving Systems 2.0

ISO/TS 22726-1&2 – Intelligent Transport Systems – Dynamic Data and Map Database Specification for Connected and Automated Driving System Applications – Part 1: Architecture and Logical Data Model for Harmonization of Static Map Data

BSI PAS 1883:2020 – Operational Design Domains for Safe Automated Driving

ISO/TR 22086-1:2020 – Intelligent Transport Systems (ITS) – Network Based Precise Positioning Infrastructure for Land Transportation – Part 1: General Information and Use Case Definitions

ISO/TR 20529-1:2017 – Intelligent Transport Systems – Framework for Green ITS (G-ITS) Standards – Part 1: General Information and Use Case Definitions

ISO/TC 204 – Intelligent Transportation Systems Technical Committee

ISO AWI TR 23254 – Intelligent Transport Systems – Architecture – Use Cases and High-Level Reference Architecture for Connected, Automated Vehicles

ISO/CEN 17380 – Intelligent Transport Systems – Urban-ITS – "Controlled Zone" Management for Uvars Using C-ITS

ISO/DIS 20529-2 – Intelligent Transport Systems – Framework for Green ITS (G-ITS) Standards – Part 2: Integrated Mobile Service Applications

ISO/WD 34503 – Road Vehicles – Taxonomy for Operational Design Domain for Automated Driving Systems

ISO/WD TS 14813 – Intelligent Transport Systems – Reference Model Architecture(S) for the ITS Sector – Part 1: ITS Service Domains, Service Groups and Services

ISO/PWI 24318 – Intelligent Transport Systems – Mobility Integration – Architecture for Automation

ISO/PWI 24315 – Intelligent Transport Systems – Management for Electronic Traffic Regulations (METR) – Part 1: General Concept and Architecture

ISOA PAS 21448:2019 – Road Vehicles – Safety of the Intended Functionality

ISO/TS 19091:2019 – Intelligent Transport Systems – Cooperative ITS – Using V2I and I2V Communications for Applications Related to Signalized Intersections

MUSICC Scenario Database and Definition Language

NEMA TS 10 – Connected Vehicle Infrastructure—Roadside Equipment

NTCIP 1211 V02 – Object Definitions for Signal Control and Prioritization (SCP)

BSI PAS 1883 – Operational Design Domain (ODD) Taxonomy for an Automated Driving System (ADS)

SAE J1698 – Event Data Recorder

SAE J2735SET – V2X Communications Message Set Dictionary™ Set

SAE J3161 – C-V2X Deployment Profiles

SAE J3186 – Application Protocol and Requirements for Maneuver Sharing and Coordinating Service

SAE J3224 – V2X Sensor-Sharing for Cooperative & Automated Driving

SAE J2944 – Operational Definitions of Driving Performance Measures and Statistics

SAE J2945/B - Recommended Practices for Signalized Intersection Applications

B.2 Physical Infrastructure

Manual on Uniform Traffic Control Devices

TAC Manual on Uniform Traffic Control Devices for Canada

TAC Geometric Design Guide for Canadian Roads

TAC Safety Performance of Bicycle Infrastructure

TAC Pedestrian Crossing Control Guide

TAC Canadian Model Rules of the Road

TAC Canadian Guide to Traffic Calming

TAC Application Guidelines for Speed Display Devices

TAC Canadian Roundabout Design Guide

TAC National Guidelines for Work Zone Safety in Canada

TAC Sign Pattern Manual

TAC Speed Management Guide: A Book in the Canadian Road Safety Engineering Handbook

TAC Digital and Projected Advertising Displays: Regulatory and Road Safety Assessment Guidelines

TAC Primer: Truck Lanes in Canadian Urban Areas

TAC Traffic Signal and Pedestrian Signal Head Warrant Handbook

TAC Traffic Signal Guidelines for Bicycles

TAC Pavement Asset Design and Management Guide

TAC Roadway Lighting Efficiency and Power Reduction Guide

TAC Synthesis of Practices of Geometric Design for Special Roads

TAC Guidelines for Selecting Sign Sheeting to Meet Minimum Retroreflectivity Levels

TAC Guidelines on the Use and Installation of Chevron Alignment Signs

TAC Bikeway Traffic Control Guidelines for Canada

TAC Recommended Practices for LED-Embedded Traffic Signs (LETS)

TAC Recommended Practices for Posting Ramp Speeds

TAC Guidelines for the Application and Display of Transit Signals

TAC Developing and Managing Transportation Infrastructure in Permafrost Regions

TAC Synthesis of Practices for Median Design

TAC Guide to Bridge Traffic and Combination Barriers

TAC Guidelines for the Planning, Design, Operation and Evaluation of Reversible Lane Systems

TAC Canadian Guidelines for Establishing Posted Speed Limits

TAC Road Safety Engineering Management Guide: A Book in the Canadian Road Safety Engineering Handbook (CRaSH)

TAC Guidelines for the Application and Implementation of the School Bus Stop Ahead (WC-9) Sign

TAC Synthesis of Current Practices for Enhancing Traffic Signal Conspicuity

TAC Guidelines for Understanding, Use and Implementation of Accessible Pedestrian Signals

TAC Guide for Lateral and Vertical Roadside Sign Placement

TAC Canadian Capacity Guide for Signalized Intersections

TAC Handbook of Recommended Information Sign Symbols for Canada

TAC School and Playground Areas and Zones: Guidelines for Application and Implementation

TAC Guide for the Design of Roadway Lighting

TAC Synthesis of Practices for Work Zone Speed Management

TAC Canadian Traffic Signal Warrant Matrix Procedure

TAC Advance Warning Flashers: Guidelines for Application and Installation

TAC Best Practice Guidelines for the Design and Application of Transverse Rumble Strips

TAC National Guide to Erosion and Sediment Control on Roadways Projects

TAC Supplemental Guide for Guide and Information Signage in Canada

TAC Illumination of Isolated Rural Intersections

TAC Design Vehicle Dimensions for Use in Geometric Design

Ontario O Reg. 239/02: Minimum Maintenance Standards for Municipal Highways

Ontario Traffic Manual

New Brunswick Motor Vehicle Act – Traffic Control Devices

Quebec Volume V – Traffic Control Devices

Nova Scotia Motor Vehicle Act section 88 – Traffic Sign Regulations

ISO 20684-10: Roadside Modules SNMP Data Interface. Part 10: Variable Message Signs

American Association of State Highway and Transportation Officials (AASHTO) A Policy on Geometric Design of Highways and Streets (Green Book)

AASHTO Bridge Design Specifications

AASHTO Guide for the Development of Bicycle Facilities

AASHTO Guide for Geometric Design of Transit Facilities on Highways and Streets

AASHTO Guide for the Planning, Design, and Operation of Pedestrian Facilities (Expected Soon)

AASHTO Guidelines for Geometric Design of Low-Volume Roads

AASHTO Highway Safety Manual

AASHTO Maintenance Manual for Roadways and Bridges

AASHTO Manual for Assessing Safety Hardware (MASH)

AASHTO Pavement Management Guide

AASHTO Roadside Design Guide

ISO 2575-2010: Road Vehicles – Symbols for Controls, Indicators, and Tell-Tales

ITE TMDD Guide TMDD & MS/ETMCC Guide Standard for Functional Level Traffic Management Data Dictionary (TMDD) and Message Sets for External Traffic Management Center Communications

ITE TMDD 3.3 ITE TMDD Traffic Management Data Dictionary (TMDD) Standard for Center to Center Communications

NACTO Blueprint for Autonomous Urbanism

NACTO Urban Street Design Guide

NACTO Transit Street Design Guide

NACTO Global Street Design Guide

NACTO Urban Bikeway Design Guide

NTCIP 8005 NTCIP 8005 Process, Control and Information Management Policy

NTCIP 1213 Object Definitions for Electrical and Lighting Management Systems (ELMS)

NTCIP 9001 NTCIP Guide

NTCIP 2306 Application Profile for XML Message Encoding and Transport in ITS Center-to-Center Communications (C2C XML)

NTCIP 9012 Testing Guide for Users

NTCIP 8007 Testing and Conformity Assessment Documentation within NTCIP Standards Publications

NTCIP 9010 XML in ITS Center-to-Center Communications

NTCIP 1211 Object Definitions for Signal Control and Prioritization (SCP)

NTCIP 8004 Structure and Identification of Management Information

NTCIP 2201 Transportation Transport Profile

NTCIP 2304 Application Profile for DATEX-ASN (AP-DATEX)

NTCIP 2303 File Transfer Protocol (FTP) Application Profile

NTCIP 2301 Simple Transportation Management Framework (STMF) Application Profile;

NTCIP 2302 Trivial File Transfer Protocol (TFTP) Application Profile

NTCIP 1102 Octet Encoding Rules (OER) Base Protocol

NTCIP 1104 Center-to-Center Naming Convention Specification

NTCIP 1205 Object Definitions for Closed Circuit Television (CCTV) Camera Control;

NTCIP 1201 Global Object Definitions

NTCIP 2202 Internet (TCP/IP and UDP/IP) Transport Profile

NTCIP 1209 Data Element Definitions for Transportation Sensor Systems (TSS)

NTCIP 1202 Object Definitions for Actuated Traffic Signal Controller (ASC) Units

NTCIP 1206 Object Definitions for Data Collection and Monitoring (DCM) Devices

NTCIP 1203 Object Definitions for Dynamic Message Signs (DMS)

NTCIP 1204 Object Definitions for Environmental Sensor Stations (ESS)

NTCIP 1208 Object Definitions for Closed Circuit Television (CCTV) Switching

NTCIP 1210 Field Management Stations (FMS) – Part 1: Object Definitions for Signal System Masters

NTCIP 2101 Point to Multi-Point Protocol Using RS-232 Subnetwork Profile

NTCIP 8003 Profile Framework

NTCIP 1207 Object Definitions for Ramp Meter Control (RMC) Units

NTCIP 1101 Simple Transportation Management Framework (STMF)

NTCIP 1103 Transportation Management Protocols (TMP)

NTCIP 2103 Point-to-Point Protocol over RS-232 Subnetwork Profile

NTCIP 2104 Ethernet Subnetwork Profile

NTCIP 2102 Point to Multi-Point Protocol Using FSK Modem Subnetwork Profile

NTCIP 1218 v01 Object Definitions for Roadside Units (RSUs)

ITE RSU Standardization

ITE Infrastructure Standards Security Assessment

ATC 5201 (ITE ATC Controller) Advanced Transportation Controller (ATC)

ITE ATC API Application Programming Interface (API) Standard for the Advanced Transportation Controller (ATC)

ATC 5301 Advanced Transportation Controller (ATC) Cabinet Version 02

ATC 5202 (ITE ATC Type 2070) Model 2070 Controller Standard

ITE LED Circular Signal Supplement Purchase Specification

ITE Vehicle Traffic Control Signal Heads – Part 3: Light Emitting Diode (LED) Vehicle Arrow Signal Modules

ITE Traffic Engineering Handbook

ITE Pedestrian Traffic Control Signal Indicators-Light Emitting Diode (LED) Signal Modules

ITE Preemption of Traffic Signals Near Railroad Crossings

ITE Guidelines for Determining Traffic Signal Change and Clearance Intervals

APTA AC-GSM-RP-001-10 – Developing a Gap Safety Management Program

APTA BTS-BRT-RP-005-10 – Implementing Bus Rapid Transit Intelligent Transportation Systems

ADA Accessibility Guidelines

B.3 Cybersecurity and Data Privacy

PAS 1885 [emerging] – Fundamental Principles of Automotive Cybersecurity Specifications

ISO 21434 [emerging] – Joint Document with SAE – Road Vehicles Cybersecurity Engineering

ISO 24089 [emerging] – Software Update Engineering

ISO/PAS 5112 [emerging] – Guidelines for Auditing Cybersecurity Engineering

ISO TR 4804 [emerging] – Safety and Cybersecurity for Automated Driving Systems – Design, Verification and Validation

AutoSAR – Specification for Secure Onboard Communication

Canada’s Vehicle Cyber Security Guidance

NHTSA Cybersecurity Best Practices for Modern Vehicles

PIPEDA

California Consumer Privacy Act of 2018 (CCPA)

SELF DRIVE ACT [not enacted]

AV START ACT [not enacted]

SAE J3101 – Hardware Protected Security for Ground Vehicles

SAE J3061 – Cybersecurity Guidebook for Cyber-Physical Vehicle System

SAE J3061-1 [emerging] – Automotive Cybersecurity Integrity Level (ACsIL)

SAE J3061-2 [emerging] – Security Testing Methods

SAE J3061-3 [emerging] – Security Testing ToolsUNECE TFCS – Cyber and OTA Software

WP.29 UN Regulation No. 155 – Cyber Security and Cyber Security Management System

WP.29 UN Regulation No. 156 – Software Update and Software Update Management System

UNECE WP. 29 [emerging] – Technical Requirements for Cyber Security and Software Updates

EU General Data Protection Regulation (GDPR)

ISO 27035 – Information Security Incident Management

ISO/IEC 29147: 2018 – Information Technology – Security Techniques – Vulnerability Disclosure

ISO/IEC 30111: 2019 – Information Technology-Security Techniques – Vulnerability Handling Processes

PAS 11281:2018 – Connected Automotive Ecosystems. Impact of Security on Safety. Code of Practice

National Motor Freight Traffic Association RFP Templates: Appendix II Cyber Security Requirements

Automotive Information Sharing and Analysis Centre (Auto-ISAC) Automotive Cybersecurity Best Practices – Key Cybersecurity Functions (2019)

Chennakeshu, Sandeep. Blackberry. Cybersecurity for Automobiles: BlackBerry’s 7-Pillar Recommendation (December 2017)

European Automobile Manufacturers Association’s (ACEA) Principles of Automobile CyberSecurity (2017)

European Union Agency for Cybersecurity (ENISA) Good Practices for Security of SmartCars (November 2019)

United Kingdom’s Department for Transport (DfT) and the Centre for the Protection of National Infrastructure (CPNI) – The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles (October 2016)

OpenXSAM [emerging] – Open XML Security – Security Analysis Model

CS-JP [emerging] – Cybersecurity Updates and Guidelines

China – SAC/TC114/SC34 [emerging] – Cybersecurity for the Driving Environment Perception and Early Warning, Driving Assistance, Automatic Driving, and Onboard Information Services Directly Related to Car Driving

SAE 1939-91C [emerging] – Network Security

ISO 14229-1 [emerging] – Unified Diagnostic Services (UDS) – Part 1: Application Layer

SAE J3005-2 [emerging] – Permanently or Semi-Permanently Installed Diagnostic Communication Devices, Security Guidelines

ETSI TS 102 731 – ITS Security Services and Architecture

SAE J1979 – Electronic and Electrical Components and Units Diagnostic Test Modes

SAE J3138 – Diagnostic Link Connector Security

ISO 15765-5 [emerging] – Diagnostic Communication over Controller Area Network (Docan) – Part 5: Specification for an In-Vehicle Network Connected to the Diagnostic Link Connector

ISO 20080 – Information for Remote Diagnostic Support – General Requirements, Definitions and Use Cases

ISO 20078-4 – Extended Vehicle (ExVe) Web Services – Part 4: Control

ISO 27001 – Information Security Management

ETSI TS 102 941 – ITS Trust and Privacy Management

ETSI TR 102 893 – Threat, Vulnerability and Risk Analysis (TVRA)

National Institute of Standards and Technology (NIST) Cybersecurity Framework

Technical Reference 68-3 – Singapore Standards Council

SAE 1939-91A – CAN Bus Protocol Network Security

SAE J1939-91B – Network Security for OTA, ExVe and ITS

IEEE 802.11 – Wireless Local Area Networks

IEEE 1609.2.1 [emerging] – Wireless Access in Vehicular Environments (WAVE) – Certificate Management Interfaces for End Entities

ASTM E2213-03 – Standard Specification for Telecommunications and Information Exchange between Roadside and Vehicle Systems – 5-GHz Band Dedicated Short-Range Communications (DSRC), Medium Access Control (MAC), and Physical Layer (PHY) Specifications

SAE J2354 – Message Sets for Advanced Traveler Information System (ATIS)

ETSI TS 102 940 – ITS Communications Security Architecture and Security Management

ETSI TR 103 630 – Pre-standardization Study on ITS Facility Layer Security for C-ITS Communication Using Cellular Uu Interface

CSA Group Research

In order to encourage the use of consensus-based standards solutions to promote safety and encourage innovation, CSA Group supports and conducts research in areas that address new or emerging industries, as well as topics and issues that impact a broad base of current and potential stakeholders. The output of our research programs will support the development of future standards solutions, provide interim guidance to industries on the development and adoption of new technologies, and help to demonstrate our on-going commitment to building a better, safer, more sustainable world.

CSA GROUP™