NIST Internal Report
NIST IR 8527

Standards and Performance Metrics for On-Road Automated Vehicles

Craig I. Schlenoff
Zeid Kootbally
Prem K. Rachakonda
Suzanne Lightman
Apostol T. Vassilev
David A. Wollman
Edward R. Griffor

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8527

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Internal Report
NIST IR 8527

Standards and Performance Metrics for On-Road Automated Vehicles

Craig I. Schlenoff
Zeid Kootbally
Prem K. Rachakonda
Engineering Laboratory

Suzanne Lightman
Apostol T. Vassilev
Information Technology Laboratory

David A. Wollman
Edward R. Griffor
Communications Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8527

June 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

Publication History
Approved by the NIST Editorial Review Board on 2024-06-03

How to cite this NIST Technical Series Publication:
Schlenoff C, Kootbally Z, Rachakonda P, Lightman S, Vassilev A, Wollman D, Griffor E () Standards and Performance Metrics for On-Road Automated Vehicles. (National Institute of Standards and Technology, Gaithersburg, MD), NIST IR 8527. https://doi.org/10.6028/NIST.IR.8527

Author ORCID iDs
Craig I. Schlenoff: 0000-0001-5899-7024
Zeid Kootbally: 0000-0001-6323-1824
Prem K. Rachakonda: 0009-0007-5290-4430
Suzanne Lightman: 0000-0002-5007-3887
Apostol T. Vassilev: 0000-0002-9081-3042
David A. Wollman: 0000-0002-6843-3692
Edward R. Griffor: 0000-0001-5241-7551

Contact Information
zeid.kootbally@nist.gov
100 Bureau Dr, Gaithersburg, Maryland, 20899

Abstract

On September 5–8, 2023, the National Institute of Standards and Technology (NIST) held the second Standards and Performance Metrics for On-Road Automated Vehicles Workshop. This four-day virtual event provided updates on NIST's recent work in automated vehicles (AVs) and gave stakeholders an opportunity to provide feedback and input on current and future NIST research. The workshop included high-level keynote presentations, a series of industry keynote presentations, and NIST presentations on its current AV activities. The industry keynotes and NIST presentations were paired with breakout sessions that discussed NIST's progress, community challenges, and stakeholder research needs in six key areas: systems interaction, perception, cybersecurity, communications, artificial intelligence, and digital infrastructure. There was general agreement that developing standards allows for better comparisons and evaluations of emerging technologies. Other key themes included: 1) Digital technologies for automation and related security/privacy concerns, including artificial intelligence, machine learning, and smart communication technologies (i.e., vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X)); 2) Need for standardized or common language to improve information sharing; 3) Open data sets to support and validate technical advances and standardization across system components and areas (i.e., standards evolving in parallel with technology); and 4) Pivotal role for NIST as a convener to bring diverse stakeholders together for knowledge exchange and cross-industry dialogue.

Keywords

artificial intelligence; automated vehicle; automotive; autonomous; communications; cybersecurity; perception; safety; sensing; transportation; V2X.

Table of Contents

List of Tables

List of Figures

Preface

On September 5–8, 2023, the National Institute of Standards and Technology (NIST) held the second Standards and Performance Metrics for On-Road Automated Vehicles Workshop. This four-day virtual event provided updates on NIST's recent work in automated vehicles (AVs) and gave stakeholders an opportunity to provide feedback and input on NIST's progress, industry challenges, and research needs. This report provides a summary of the workshop findings.

Acknowledgments

Thanks are extended to the NIST workshop organizers for bringing participants together, presenting materials on technical topics, and guiding discussions. Craig I. Schlenoff led the NIST Strategic and Emerging Research Initiatives (SERI)-funded AV effort at the time of the workshop and also served as master of ceremony. In addition, the broader NIST Automated Vehicles team members are thanked for their help with contributing to NIST presentations and organizing and answering questions at the breakout sessions.

Workshop Organizers

Workshop Lead:	Craig I. Schlenoff
Systems Interaction:	Zeid Kootbally
Perception:	Prem K. Rachakonda
Cybersecurity:	Suzanne Lightman
Communications:	David A. Wollman
Artificial Intelligence:	Apostol T. Vassilev
Infrastructure:	Edward R. Griffor

NIST also wishes to thank the speakers for providing perspectives on various topics and effectively setting the stage for discussions.

Keynote and Plenary Speakers

Keynote:	Ann E. Carlson (Acting Administrator, NHTSA)
Systems Interaction:	David Agnew (VP Business Development, Dataspeed Inc.)
Perception:	Rajeev Thakur (SAE Instructor for LiDAR and Infrared camera technologies)
Communications:	Jim Misener (Global V2X Ecosystem Lead, Qualcomm)
Artificial Intelligence:	Aleksander Madry (Director of the Center for Deployable Machine Learning, MIT and research staff at OpenAI)
Cybersecurity:	Anuja Sonalker (CEO and co-founder of STEER)
Infrastructure:	Session Keynote Overview – Ed Straub (VP and Director of Automation Office at SAE) and Kelley Coyner (Leidos) Industry Keynote Overview – Jeffrey Wishart (Fellow at the Science Foundation of Arizona), Michael Mollenhauer (Director of Technology Implementation at VTTI), Henry Liu (Director of CCAT), and Craig Hinners (Intelligent Transportation Systems (ITS) Solutions Architect at NoTraffic)

Author Contributions

Craig I. Schlenoff: Supervision. **Zeid Kootbally**: Software, Writing, Reviewing, and Editing. **Prem K. Rachakonda**: Supervision. **Suzanne Lightman**: Writing, Reviewing, and Editing. **Apostol T. Vassilev**: Writing, Reviewing, and Editing. **David A. Wollman**: Writing, Reviewing, and Editing. **Edward R. Griffor**: Writing, Reviewing, and Editing.

1. Introduction

On-road automated vehicles (AVs) are expected to significantly influence daily life. However, these complex systems can pose safety risks in the event of unexpected system performance. In March 2022, the National Institute of Standards and Technology (NIST) held the Standards and Performance Metrics for On-Road Autonomous Vehicles Workshop to solicit stakeholder feedback on challenges and opportunities in developing standards and performance metrics for this complex, interdisciplinary field. The output of the workshop [1] identified a number of key areas in which NIST can support the AV community.

Throughout 2023, NIST researched performance metrics and standards for several targeted areas. As part of these activities, NIST held a workshop on September 5–8, 2023, to provide updates on progress, gain feedback, gather ideas from the AV community, and initiate discussions on infrastructure needs for on-road vehicles, which is a relatively new area of research for NIST.

The workshop included a series of plenary sessions and an overall keynote speaker — Ann E. Carlson, Acting Administrator of the National Highway Traffic Safety Administration — who highlighted the Biden Administration's AV safety initiatives and NIST's efforts in AV measurement. In the following sessions, NIST AV project leads provided updates on industry perspectives and NIST's recent work in the area, which was motivated by stakeholder input during the 2022 AV workshop. Each NIST presentation was coupled with an industry keynote address and followed by a breakout session to gather information from stakeholders on challenges and future Research and Development (R&D) needs. These ideas will help NIST ensure that future efforts toward standards and performance metrics provide the greatest value to the AV community.

The virtual four-day workshop drew over 600 attendees, including experts in the field from industry (over 40 % of attendees), academia ($\sim$20 %), the Federal Government ($\sim$17 %), state and local governments ($\sim$7 %), research organizations, not-for-profit organizations, accreditation bodies, standards development organizations, financial firms, technical consulting firms, and various other organizations.

This report provides a summary of the work presented by NIST and the subsequent discussions that took place during the workshop, exploring the following topic areas:

- Systems Interaction: Frameworks will be needed to evaluate the specific interactions that occur between systems and components, such as sensors and communication. NIST has developed initial simulations for a systems interaction testbed.
- Perception: AV perception and sensing communicate and interpret information about the vehicle's environment, the objects around it, and people using computing hardware and software to plan responses. NIST is developing a perception testbed and evaluation methods using International Systems of Units (SI) traceable artifacts.

- Cybersecurity: Cybersecurity for AVs involves measures to safeguard information and protect vehicles from hackers or those attempting to gain access to AV intellectual property. Machine learning (ML) and artificial intelligence (AI) add additional unique security considerations. NIST has established an Automotive Cybersecurity Community of Interest to inform industry stakeholders about NIST cybersecurity work that is relevant to AVs.
- Communications: Communication networks are closely linked to a vehicle's awareness of its operating environment and its ability to react to unsafe operating conditions. NIST is evaluating AV communications requirements, developing network modeling capabilities, and integrating the models into an AV co-simulation and systems interaction testbed.
- Artificial Intelligence: AI and ML enable AVs to navigate and operate on their own. NIST is developing a capability to estimate uncertainties related to the use of AI for object recognition and classification and machine learning models, including producing a taxonomy of terminology and attacks in adversarial ML.
- Infrastructure: An array of roadway infrastructure systems will be needed to collect, interpret, and transmit signals to AVs on elements such as traffic, construction, road conditions, and other vital conditions. NIST has partnered with several state Departments of Transportation, the SAE International standards organization, and others to explore requirements for future traffic infrastructure.

2. Keynote and Plenary Speakers

U.S. Congresswoman Haley Stevens (U.S. representative from Michigan's 11th congressional district) and Hannah Brown (NIST Deputy Associate Director of Laboratory Programs) provided welcoming remarks that focused on the importance of developing standards for AVs and thanked the broad range of experts for attending and providing their perspectives.

Plenary speakers gave presentations on key technical topics, which are summarized in the following section and can be found online for a limited time (see Appendix H).

Jayne Morrow, NIST Senior Advisor for Standards Policy — U.S. Government National Standards Strategy for Critical and Emerging Technology (USG NSSCET)

Jayne Morrow is a Senior Advisor to the Director of NIST and leads the development of standards policies for critical and emerging technologies. Dr. Morrow discussed the U.S. Government National Standards Strategy for Critical and Emerging Technologies (White House 2023), which has identified critical and emerging technology sectors (e.g., automotive and connected transportation, AI, semiconductors, renewable energy) that require collaboration across academia, government, and industry to dynamically develop standards. The strategy involves four major objectives:

- Investment (and the role of R&D in supporting standards).
- Participation (including a need for additional subject-matter experts to participate in standards development processes).
- Workforce (addressing the need for long-term sustainability of Science and Technology (S&T) workforce).
- Integrity and Inclusivity (promoting stronger relationships with global partners and sustaining the integrity of standards).

Dr. Morrow emphasized the importance of feedback from stakeholder communities on both the technologies themselves and strategies for aligning U.S. standards development organizations with applicable industries, non-governmental organizations (NGOs), academia, and foreign governments. Stakeholders can participate through scheduled events, the Standards.gov website https://www.nist.gov/standards.gov, and responding to requests for information (RFIs), which invite ideas, recommendations, and suggestions on ways that the U.S. Government can better support the work of the National Standards Strategy for Critical and Emerging Technologies. The August 2023 RFI [2] covered a few main topics, such as workforce and investments.

Ann E. Carlson, Acting Administrator, NHTSA — NHTSA Activities

Ann E. Carlson is the Acting Administrator of the National Highway Traffic Safety Administration (NHTSA), which sets standards, identifies defects, manages recalls, and administers millions of dollars in grants to state highway safety offices. She previously served as NHTSA's Chief Council and played a critical role in advancing the agency's safety mission. During her presentation, Ms. Carlson emphasized the importance of technology — specifically automation — to promote safety and enhance driver comfort, including tools like automatic emergency braking (AEB). She also discussed NHTSA legal authorities beyond enforcement, such as issuing exemptions for automated vehicles under Section 30113 and 30114 of the Vehicle Safety Act.

NHTSA's current work focuses on safety issues, such as requiring vehicle design changes, addressing risky driving behaviors, and improving 911 services. For example, NHTSA has drafted and proposed a rule to require AEB (along with three other technologies) to the New Car Assessment Program (NCAP). NHTSA's standing general order also requires crash and incident reports for vehicles equipped with an automated driving system (ADS). This material is available to the public at https://www.nhtsa.gov/sites/nhtsa.gov/files/2023-04/Second-Amended-SGO-2021-01_2023-04-05_2.pdf (NHTSA 2023). In addition, under Section 30114, NHTSA is working on proposed rulemaking for a new program called the ADS-equipped Vehicle Safety, Transparency and Evaluation Program (AV STEP).

NHTSA has some rulemaking authority with respect to ADS. The first ADS-related rule was released in 2021, and NHTSA will likely work further to develop a regulatory structure for automated vehicles. NHTSA has also established the Office of Automation Safety under

their existing Office of Rulemaking, which is responsible for actions such as developing the next set of standards. Under its enforcement authority, NHTSA could publish ADS rulemaking on the safety of occupants and seek rulings for manufacturer accountability. In the future, NHTSA plans to relaunch the Automated Vehicle Transparency and Engagement for Safe Testing Initiative (AV TEST) — an online tracking tool where the public can learn about the testing and development of ADS vehicles.

Craig I. Schlenoff, NIST — Overview of 2022 Workshop and Relevant NIST Activities

Craig I. Schlenoff, NIST Program Manager of Robotic Systems for Smart Manufacturing, provided background on the 2022 Standards and Performance Metrics for On-Road Autonomous Vehicles Workshop and the NIST activities that were generated as a result. During the 2022 workshop, NIST conducted over 60 one-on-one interviews with stakeholders and facilitated four focus group meetings with domain experts. The workshop outputs are summarized in a NIST publication [1].

Throughout 2023, NIST researched and explored performance metrics and standards in a number of the key areas, including AI, communications, cybersecurity, perception, and systems interaction. Further analysis of potential impacts, industry needs, and NIST expertise informed the focus areas for the 2023 workshop. NIST has since initiated work on system-level testing (e.g., assessing automotive sensor perception, minimizing risk in AI, measure cybersecurity, and evaluating communication technologies) and is conducting systems interaction testing via a testbed to facilitate the measurement of system interaction when perturbations are introduced into the system under controlled conditions.

3. Systems Interaction

3.1. Industry Keynote Overview

David Agnew, Vice President, Business Development, Dataspeed Inc. — The Operational Domain and the Human Driver as the Baseline for AV Metrics

David Agnew presented on systems interaction with an overview of autonomous vehicle (AV[1]) and human performance metrics, including the metrics of car crashes versus domestic fatalities. The primary discussion points involved the need to effectively measure AV performance, highlight the significant aspects of crashes involved in driving, and benchmark AV performance to human driver safety performance to establish a baseline for comparison. The metric used for U.S. human safety performance is the total annual miles driven per total fatalities based on 2022 NHTSA data, which is currently 73 million miles/fatality. The goal is to reduce human fatalities by increasing the number of miles

[1]While NIST uses the term "automated vehicle" to refer to a vehicle under human operation that contains one or more automated features, Mr. Agnew's presentation explicitly used the term "autonomous vehicles". All references to autonomous vehicles in this section are intentional to reflect the language used by the speaker.

driven between fatal mishaps. AV safety performance intends to eliminate 90 % of accidents by increasing the target for AV human safety performance to 730 million miles. The benchmarking of AV to human safety performance targets can potentially be derived from simulations given credible methodologies as they are developed.

3.2. Scope

Two main approaches are currently used for testing AVs:

- System-level (or component) testing pertains to the testing of components in isolation from their surroundings.
- Full-system testing evaluates the performance of AVs within an environment (e.g., other vehicles, pedestrians, roadway obstacles of equipment, etc).

Systems interaction covers the scope of individual systems interacting within the vehicle and full vehicle systems operations in the driving/roadway environment. Systems interaction could include communication (e.g., data exchange modules) interacting with perception (i.e., sensor) systems. Systems interactions involve many different types of software and hardware and can be quite complex.

NIST has been researching systems interactions with a focus on developing a physical and virtual (i.e., simulation) testbed to transition individual system-level testing to overall vehicle performance. The reproducible systems interaction testbed uses measurement science and standards to assess AVs. The approach begins with simulations, followed by laboratory implementation and tracking of testing with partner institutions. The testbed incorporates multiple elements, including the design of an AV system's interaction architecture and implementation of that architecture to study on-road scenarios using the Automated Driving Systems Interaction (ADSIE) framework. The ADSIE framework enables stakeholders to create, evaluate, and implement testing scenarios aimed at capturing the system interaction performance of automated driving features. The systems interaction architecture is under active development as part of NIST's research efforts, and these diagrams will continue to be refined.

The simulation infrastructure for a systems interaction testbed allows for example scenarios of the ADSIE framework. This simulation testbed is intended to be used by stakeholders for evaluation, and its infrastructure consists of the following:

- Driving scenarios and environments with CARLA (https://carla.org/).
- Automated driving functions operated by Autoware (https://autoware.org/).
- Flexible software publish/subscribe messaging using ROS (https://www.ros.org/).
- Vehicle-to-everything (V2X) communication managed by the ns-3 network simulator (https://www.nsnam.org/).

Through this testbed, NIST can provide driving scenarios and capture the corresponding metrics to demonstrate the feasibility and value of studying systems interaction. This simulation testbed is also meant to transition to hardware testing setups for physical systems interaction testing.

This discussion session focused on:

- Gaining feedback on current NIST research and testbed activities.
- Understanding current and future measurement, testing, and standardization challenges to safe, reliable system interactions, both internally and externally to the vehicle.
- Identifying approaches and needs for future R&D and testing.

3.3. Feedback on Current Programs and Activities

Progress at NIST toward developing a systems interaction testbed and architecture (Fig. 1) was presented in the form of a framework diagram. Overall feedback on the diagram and testbed approach was positive, and it was noted as being comprehensive and inclusive of the necessary elements. The diagram's primary attributes include its relational form (and thinking), clear definition of interactions between components, and graphic visualization of different components and their interconnections. This framework diagram has since been improved by NIST.

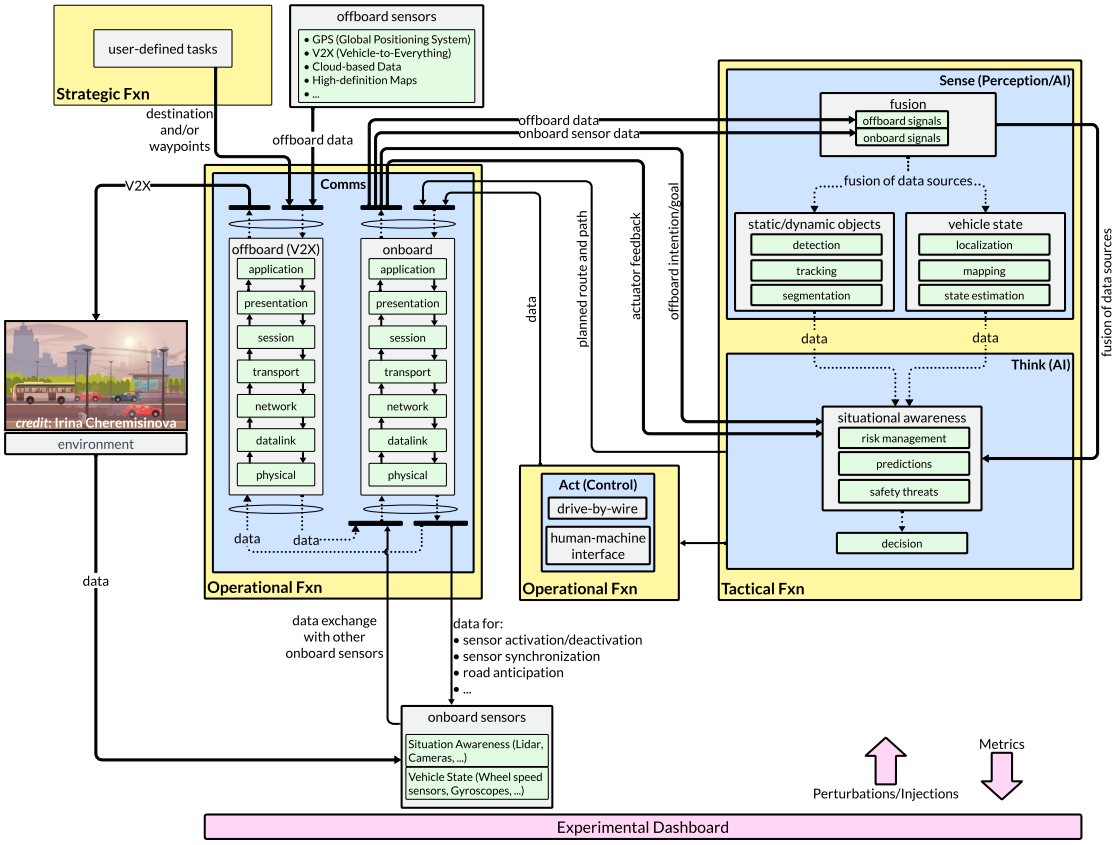

Fig. 1. Systems interaction architecture.

The complexity of the diagram was called out as a challenge with potential for simplification. General comments noted that AVs are still in a nascent stage. Since few are on the road, the architecture is currently sufficient. However, as more AVs are launched throughout the United States, new challenges will rapidly emerge, and system levels may need to be added. Hence, the architecture should be dynamic and amenable to adjustments. Appendix C provides a summary of comments and proposed improvements and adjustments.

3.4. Identification of Challenges

A number of challenges were identified that impact effectively mapping, testing, and evaluating systems interactions within the AV and external to the environment. Common challenges included the lack of standardization across system interfaces, the inability to safely test in real-world environments, processing and analyzing the enormous data sets generated by AV systems, and the lack of open data sets to support models, simulations, and testing criteria. Accessible testbeds are also lacking, and there is insufficient data to test for solutions. The need to protect intellectual property exacerbates these issues since

Original Equipment Manufacturer (OEM) data and networks are monetized and generally inaccessible due to proprietary concerns.

Table 10 (from Appendix C) summarizes the challenges.

3.5. Approaches and Needs for Research and Testing

Several major topics for research and testing were identified, ranging from unusual scenario analysis to interoperability testing and sensor development and fusion. Common themes for key metrics for co-simulation architecture and the documentation of interaction results are summarized in Table 11 (Appendix C).

Testing and capturing how AV systems interact was considered essential, as vital research and related testing are necessary to transition AVs into mainstream use. European projects, such as PEGASUS[2], could be reviewed to compare scenario testing methods, metrics, and proposed operational design domains (ODDs) for automation. A recommendation was made for NIST to develop a prioritized list of the critical scenarios to be considered for testing. It was noted that the most valuable testing outcomes should be identified and understood, such as hardware interaction testing and where it could best serve the community (e.g., essential for interoperability).

Testing simulations may not uncover all issues and may need to be adjusted to be useful. The practical utility of the models should also be understood since the initial phase of deployment based on current models and simulations could have some risks or failures (with failsafe mechanisms built in). Systems interaction testing enables a better understanding of the risks that could be encountered during deployment (i.e., measured risks). The information that humans need to drive can provide the details for AV driving. Not every sign or symbol may be needed, but there are crucial pieces of information that cannot be left out. The information required for safe driving needs to be filtered from the available data to create an initial baseline.

4. Perception

4.1. Industry Keynote Overview

Rajeev Thakur, SAE Instructor for LiDAR and Infrared Camera Technologies — Perception Keynote

Rajeev Thakur discussed the complexity of AV systems, smaller companies having access to useful datasets, connecting the sensor and the logic behind it, and the time-intensive process to incorporate AV-specific infrastructure upgrades. The complexities of the AV system

[2]The PEGASUS Project for Autonomous Cars is sponsored by the German Federal Ministry of Economic Affairs and Energy. TÜV SÜD is working with 16 industrial and research partners to formulate methods and tool requirements to ensure the safety of highly autonomous driving functions. See https://www.tuvsud.com/en-us/industries/mobility-and-automotive/automotive-and-oem/autonomous-driving/pegasus-project.

arise from the uncertainty and latency present with human drivers. The need to establish common standards (i.e., NIST, SAE, ISO) to communicate testing is crucial, as OEMs are occupied with developing and competing in the market. Furthermore, NIST and other policy bodies should play a significant role in bringing safety and convenient AVs to society.

4.2. Scope

An AV uses sensors to stand in for humans in sense-think-act activities, such as sensing and communicating information about the environment, objects, and people; using computing hardware and software to interpret the data communicated by the sensors and plan a strategy; and using actuation hardware to respond. Measuring performance in each of these components is critical to improving the quality and safety of AVs, and industry has asked NIST to develop measurement science to help make AVs safer.

AV safety goals vary. The Automotive Safety Integrity Level (ASIL) D, an automotive risk classification, represents the highest level of risk management (ISO 26262). It currently demands a 75$\times$ improvement in vehicle safety performance (e.g., $\sim$0.02 deaths per 100 million miles at 60 mph). Tesla's calculations call for a 3–10x improvement. However, public expectations for AV performance are very high — essentially, a zero-failure rate. AV evolution is happening on the public stage, and there is little transparent discussion of failure probabilities. Unfortunately, even a 75x improvement greatly increases the costs of perception, which delays adoption.

Open discussion is needed to set realistic goals. NIST — along with the International Organization for Standardization (ISO), Society of Automotive Engineers (SAE), and other such bodies — needs to establish a common standard for communicating testing and performance. There are several parameters that affect AV sensor performance: sensor construction, operation modes, interface hardware and software, methods, targets, and environment. However, there are currently few standard test procedures to evaluate many of these parameters.

Certification tests and testing standards for AV with random scenarios are needed to support perception and other AV areas. AV hardware, software, and user experience perform well under ideal test conditions. Uncertainty with human drivers on the road, weather, sensor performance, and latencies add an order of magnitude to complexity. Testing standards for AVs must be based on the Operational Design Domain (ODD), which refers to the conditions that affect safe AV operation (e.g., roads, speed, weather, time of day/lighting, and rating evaluation). A vehicle rating of SAE Level 4 (L4) (i.e., vehicles that are nearly fully autonomous) over ODD needs to be certified by a trusted agency.

Sensor requirements and characterization standards are also critical. Sensor performance must be characterized over ODD with edge targets and in ambient conditions. Performance must then be checked in terms of range, resolution, and accuracy over limited frames. Other important considerations include the role of V2X in AV (e.g., perception

at intersections for cross-traffic) and a complete list of perception needs (e.g., signs, potholes, road debris).

Emerging technologies include thermal cameras, imaging radar, ground penetrating radar, vehicle-to-infrastructure (V2I)/vehicle-to-vehicle (V2V), and 2D Global Positioning System (GPS) barcodes in urban canyons. Existing mature technologies include Light Detection and Ranging (LiDAR), radar, visible cameras, ultrasonic, inertial measurement unit (IMU), and GPS. To analyze the LiDAR sensor technology used on AVs, NIST researchers developed a testbed in the retroreflection facility (i.e., the calibration and characterization facility), which has been upgraded to work with infrared wavelengths to support AVs. Methods were developed to evaluate sensors using SI-traceable artifacts and instrumentation, calibrated spheres that were measured using Coordinate Measuring Machine (CMMs), and a laser tracker that offers sub-millimeter uncertainties at sphere-sphere lengths $<$10 m. Researchers are evaluating how well different LiDAR sensors or combinations of sensors can "see" both spherical and planar objects (e.g., a road sign).

Several other sources of perturbation were introduced, such as retroreflective materials, angled surfaces, and ambient lighting conditions to understand the performance of LiDAR sensors in varying conditions. Researchers observed that the data acquisition software could be a source of measurement error, and the combination of certain targets (e.g., black and retro reflective targets) could lead to significant data loss on the targets. Multi-LiDAR and LiDAR-camera calibration techniques are also being explored. Initial results indicate that the LiDAR point spacing and registration algorithms can introduce significant errors when combining data from these sensors.

4.3. Feedback on Current Programs and Activities

Agreement was noted that NIST work is headed in the right direction. Developing standards — even for the basics, such as terminology and tests — allows for better comparisons and evaluations. Continuous evaluation of what is theoretically possible versus what is practically attainable is useful and has a key role in creating standards for perception sensors. Although it was noted that full standardization is still in the future, the current topics of research were seen as a good foundation for common assessment and comparison. The process will likely be iterative, with topics and challenges evolving along with new technologies. Thus, perception should be considered a "living topic".

Concerns were raised that the focus of research could be expanded. For example, NIST work concentrates on safety rather than security with limited focus on abuse of the vehicle or systems (e.g., cybersecurity attacks). Others saw current efforts as"device-centric" — that is, a strong focus on characterizing and evaluating the sensors themselves with limited engagement at the system level (e.g., with the perception algorithms that use the raw data). The focus on LiDAR was noted as a useful start but potentially too exclusive and lacking clear answers (e.g., about latency). Adding work on other mature options (e.g., radar, cameras, and hyperspectral imaging) and sensor fusion would address a broader set

of stakeholders and applications. Predictions and processing speed could also be explored to amplify reaction time.

Appendix D, Table 12 provides a summary of suggestions for additional topics and suggestions.

4.4. Identification of Challenges

A number of technical challenges were identified, including:

- Signal-to-noise ratio (SNR) situations.
- Sensor interference.
- Integration into vehicles (e.g., data overload).
- Poor sensor output.
- Limits to the number of objects that a system can detect.
- Interoperability issues.
- Ensuring that data is accurate and leads to valid information.

Appendix D, Table 13 summarizes the challenges and barriers.

Sensor combinations allow systems to leverage a range of capabilities, but fusion creates new issues, such as blind spots, blurring, and sensors contradicting each other. Certain objects that are particularly challenging in terms of detection include items in the roadway that are not normally present (e.g., animals, blown tire fragments, parts falling off cars), negative obstacles (e.g., potholes), and unrecognizable patterns (e.g., a white reflective ball, reflective and retroreflective items, color, lights, LEDs). Sensors also have an occlusion spot, where vision is obscured, and current sensor technologies function poorly in extreme weather conditions (e.g., heavy snow) and at certain times of day (e.g., night and very bright sunlight affect sensor performance).

Market barriers hinder wide-scale adoption due to the high cost of accurate perception sensors (i.e., LiDAR and cameras). Additionally, there is limited knowledge about the performance and limitations of commercially available sensors in various environments.

Small businesses, in particular, are hindered by an inability to establish a full testing environment that adequately matches real-world environments. Small businesses may not have the capital to install a closed track, sensors on a moving “vehicle”, hardware and software that can process the input, or hardware and software to send the output of the resulting reactions. Small businesses are also wary of liability concerns.

NIST could enable private-sector development by developing standards that provide practical baselines and enable comparisons between sensors. Other supportive efforts might

include a standard procedure to determine a minimum number of sensors for a set of conditions, a clear definition of "proper sensor operation", and procedures for sensor testing with known uncertainty and use results to enable the certification of system components and the systems themselves.

The prevalent approach in the industry appears to be proliferation — more wavelengths, more modulation techniques, and new sensor types. The industry is still in an exploratory phase, searching for sensors that may support perception algorithms that will be reliable across multiple ODDs. These algorithms have not matured enough to allow the industry to filter out sensor types. Consolidation may not necessarily be the right approach (and not necessary if interoperable), as complementary sensors can be leveraged for their varying limitations and strengths. Diverse sensors based on different phenomenology (i.e., different physics) are needed to provide functional redundancy in cases of environmental disturbances.

There are moves toward solid-state LiDAR (adding that mechanical detection solutions such as motor driver LiDAR are more prone to failure). Military and drone technology may also be leveraged due to recent advances in event-based cameras for automated drone flight, which is much faster than AVs. However, the work is often highly classified.

4.5. Approaches and Needs for Research and Testing

Standardization should focus on outcomes (e.g., detecting a stop sign 20 meters away) rather than sensors. Challenges are often unique to a sensor, but more generalized standards may be useful. Even non-challenging test cases can provide valuable references for more challenging conditions. Other suggestions were to explore the important sensor parameters for standardization, such as interoperability and interference issues. There is also a need for standardized minimum technical specifications (e.g., refresh rate, image quality, frame rate, range, or lag time) and minimum performance requirements (e.g., latency, false positive rates and false negative rates). Full results are summarized in Table 14 (Appendix D).

There was a strong focus on the critical roles that V2X, V2V, V2I, and AI will play in successful automation. AI systems that support AV perception should require standardization, and ways to train or improve AI in AVs should be considered. Since AI and sensor systems are evolving rapidly, specifications must be developed in parallel.

Regarding gaps, some degree of uncertainty is inevitable, and determining the acceptable level of uncertainty is essential. Common concerns also included sensor sight limitations and challenges with sensor fusion.

5. Cybersecurity

5.1. Industry Keynote Overview

Anuja Sonalker, CEO and Co-Founder of STEER — Cybersecurity

STEER develops automation technology for passenger and commercial vehicles that can be applied to parking, low-speed driving, first- and last-mile delivery, vehicle maintenance, fleet operations, and other custom use cases. Ms. Sonalker discussed how generative AI changes the cybersecurity threat landscape for AVs. Generative AI machine learning models could be used to generate new and original hacking tools based on inputs and training, making cybersecurity adversaries more dangerous if they have the financial resources and expertise to harness such tools. While less sophisticated adversaries, termed "hobby hackers", may not have the necessary expertise and resources to create and train such AIs, more advanced threats like industry competitors, criminal and terrorist networks, and hostile nation states do. Using generative AI may increase both the likelihood and impact of potential cybersecurity attacks on autonomous vehicles. The likelihood is increased by reducing the time and expertise required to hack into AV networks, providing a greater window of opportunity for potential attacks with lower equipment requirements.

Responding to these increasing threats requires a standards-based approach to developing safe and secure AV systems. This involves a standardized risk assessment method with associated levels of cybersecurity protection. It also requires continuously monitoring generative AI maturity as a tool for cybercriminals and creating associated risk metrics to counter these threats.

5.2. Scope

The significantly enhanced role of software-based systems in AVs presents numerous challenges as well as opportunities in the context of cybersecurity. Potential cybersecurity attackers of automated vehicles include hackers seeking personal gain, researchers or competitors attempting to access vehicle systems' intellectual property and internal documentation, and nation-states or terrorists with significant resources and a wide range of possible motivations. As a result, cybersecurity measures will need to incorporate varying response levels, and cybersecurity activities will need to extend far beyond the development phase of vehicles. Countermeasures and potential vehicle responses will need to be continuously incorporated to protect all system components and their interactions.

The introduction of AI and ML to achieve driving without human involvement also invokes unique considerations in terms of ensuring trustworthy vehicle operation. These include the mitigation of cybersecurity vulnerabilities and ensuring that the decision-making processes of these ML models are explainable and transparent. Further, the use of wireless software updates is a new model for this industry and can expose new attack surfaces. As

AI capabilities are introduced into AVs, coherent cybersecurity plans will have to incorporate ongoing awareness of AI's increasing capabilities to identify new attack surfaces.

NIST's Automotive Cybersecurity Community of Interest (COI)[3] was introduced in February 2023. It serves as a communication channel for industry members of the vehicle and transportation sector to engage with NIST and help identify major industry challenges and potential areas of improvement for overall cybersecurity measures as they relate to automated vehicles. This COI group currently has more than 360 members — including 17 participants from government, 20 from academia, and over 320 from industry — and 60–100 members typically attend meeting calls. Past meetings and recordings are available through NIST's Computer Security Resource Center (CSRC)[4].

NIST and its National Cybersecurity Center of Excellence (NCCoE) have been working with both the public and private sectors to effectively push industry forward into quantum-resistant cryptographic algorithms, which can better respond to the evolving threats presented by advanced quantum-computing technologies. The goal of post-quantum cryptography (PQC), also known as quantum-resistant cryptography, is to develop cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks. NIST has been engaged in processes to solicit and standardize quantum-resistant public-key cryptographic algorithms. This initiative includes efforts to identify existing quantum-vulnerable elements in vehicle systems as well as collaborate with industry partners to implement NIST-standardized, quantum-resistant systems across their product range.

This cybersecurity discussion session focused on:

- Soliciting feedback from participants about NIST's current cybersecurity efforts and other potential research areas.
- Identifying challenges that NIST initiatives could address (e.g., safety and fuel efficiency) as well as cybersecurity risks and trade-offs presented by a variety of evolving technologies.
- Identifying cybersecurity concerns and potential NIST efforts that might extend beyond automated vehicles into vehicle cybersecurity more generally.

5.3. Feedback on Current Programs and Activities

The majority of responses regarding NIST's current cybersecurity concentrations were generally positive. Other cybersecurity areas that NIST could potentially explore include physical and digital AV systems, connected devices and networks, and long-term support for software systems that stay up to date in addressing new cybersecurity threats over time.

[3] More information can be found at https://csrc.nist.gov/Projects/auto-cybersecurity-coi.
[4] AutoSec COI Presentations: https://csrc.nist.gov/Events/2023/automotive-cybersecurity-community-of-interest-2nd.

There are a handful of existing cybersecurity and vehicular standards that NIST could leverage to address AV-related concerns. NIST is already involved in a number of standards related to AVs, such as the Secure Software Development Framework (SSDF). Standards related to safety are also important to consider, such as ISO 26262 [3], ISO 21448:2022 [4], and the United Nations Economic Commission for Europe (UNECE) regulations [5] regarding cybersecurity and AVs.

Table 15 (found in Appendix E) provides a summary of the cybersecurity comments and recommendations.

5.4. Identification of Challenges

Workshop participants identified numerous challenges regarding AV systems, components, and related cybersecurity risks, as well as tentative solutions for these issues. Some major points of emphasis include concerns with how systems make decisions, fallback systems and safeguards, vulnerability to cyber attacks, and privacy concerns related to AVs' many information-intensive perception systems.

Vehicle decision-making systems are particularly vulnerable to security issues, and decision paths (particularly those powered by AI) may not be fully characterized, making effective testing more challenging. System testing and validation are key to ensuring that appropriate fail-safes and fallback modes are built into the system. The AV cybersecurity challenges are more fully detailed in Table 16 (found in Appendix E).

5.5. Approaches and Needs for Research and Testing

Discussions about vehicle cybersecurity concerns also addressed more general privacy and safety issues, including the ability of the advanced driver-assistance systems (ADAS) to exhibit cyber resiliency during incidents (e.g., hostile signal jamming, solar flares). Standards may be needed to facilitate the reporting of security incidents, blackbox monitoring for the isolation of events, and creating correlations across all vehicles on the road.

V2I communication concerns include increased awareness of vehicle connections across different platforms (e.g., cellular, WiFi, etc). Points of connection, such as interactions with transportation infrastructure and charging stations, can also be points of attack (i.e., anywhere information or data is transferred). Assurance mechanisms for GPS time will be increasingly important, and NIST has ongoing work in this area. Performance metrics are also needed for AV cybersecurity.

Table 17 (found in Appendix E) summarizes the cybersecurity comments and suggestions for future R&D.

6. Communications

6.1. Industry Keynote Overview

Jim Misener, Global V2X Ecosystem Lead, Qualcomm — Communications for Connected and Automated Vehicles

Jim Misener, Senior Director of Product Management and Global V2X Ecosystem Lead at Qualcomm Technologies, Inc., communicated the perspective of Qualcomm and their interactions with automotive customers. Qualcomm is one of a few companies with an AV stack and hardware and comprehensive vision for V2X, and their products are used in many cars and different technology domains.

Cellular-vehicle-to-everything (C-V2X) is made up of complementary transmission modes: V2I, V2V, V2P, and vehicle-to-network (V2N). The architecture of C-V2X has two complementary forms: direct actionable communication links and network communications, including backhaul connections. A current major AV constraint is the limited availability of spectrum to support intelligent transportation systems (ITS) and ITS safety in three primary geographic regions: the U.S., China, and Europe. In the U.S. and China, the spectrum for ITS (5.9 GHz band) is allocated similarly, while Europe has a larger spectrum allocation to allow for other uses. China's 2025 New Car Assessment Program (NCAP) is a driver for V2X with three basic use cases: V2V (two use cases, one for intersections and the other for long range) and V2I (use case for red light violation warnings). Europe may have an NCAP in 2029, while NHTSA has not yet finalized NCAP in the U.S., leaving the U.S. with voluntary deployment.

For the described "Day 1" deployment in the U.S., voluntary deployment will consist of a single 20 MHz channel operation that supports critical safety applications with different categorizations for traffic classes by criticality to allow for prioritized vehicle communication (V2V and V2I). IEEE 1609.2 defines security for C-V2X as authenticating the message sender through certificates (currently voluntary in the U.S.). There are future goals for cooperative perception and coordinated maneuvers where information is for vehicles and the infrastructure itself. Insufficient spectrum for both the security and protocol of sensor data sharing messages (SDSMs) remains an issue. The ultimate goal is for V2X to allow AVs to become connected and automated vehicles (CAVs).

6.2. Scope

The safe and practical operation of AVs depends on communication systems. Communication networks are closely linked with the vehicle's awareness of its operating environment and ability to react to unsafe operating conditions — functionalities contained within its ADS.

NIST has introduced the concept of an operating envelope specification (OES), which is a structured description of the operating environment for driving. The OES supports calculation-

based reasoning for vehicle performance, including testing and certification applications and real-time driving. NIST has also led an Automated Driving Systems Technical Working Group (ADS TWG) since 2020 with a focus on developing foundations for assessing AV performance. The scope of communications work at NIST covers numerous challenges related to timing and latency adequacy, testing methodology, and trustworthiness — a combination of safety, security, privacy, reliability, and resilience.

To study AV communications and evaluate system performance, simulations are being designed and developed by leveraging the existing modules in the ns-3 network simulator. ns-3 is an open-source discrete-event network simulator focused on internet and cellular systems intended primarily for research and educational use. On top of ns-3 existing modules, pluggable V2X extension modules simulate 5G New Radio (NR) cellular networks and V2X communications and incorporate fundamental PHY-MAC NR features that are aligned with the 3rd Generation Partnership Project (3GPP) NR Release 16 and comply with scenarios and channel models based on 3GPP TR 38.885.

Simulation has advantages over on-road testing because it allows for targeted, reproducible, and rapidly iterated experiments to test scenarios of interest and can cover the many failure cases that would impact people or the surrounding environment with low risk and low cost. However, pure network simulation does not provide an accurate representation of vehicle dynamics or the physical environment and must be combined with models of those domains. This can be done offline using data from sources (e.g., naturalist driving data) or online through the co-simulation of hardware and simulators that are dedicated to different domains or sub-systems. The co-simulation approach is used for NIST AV efforts to replace one or more simulated systems with physical hardware, such as a vehicle with a complete automated driving stack.

AVs have many systems working together in the driving environment that must be synchronized, optimized, and tested for performance and reliability (Fig. 2). These include onboard vehicle communications and external networks that carry communication signals. The 3GPP brings together global Standards Development Organizations (SDOs) to develop technical specifications for future generations of AV mobile/cellular telecommunication applications. Optimized AV communications with infrastructure and the external environment will be critical.

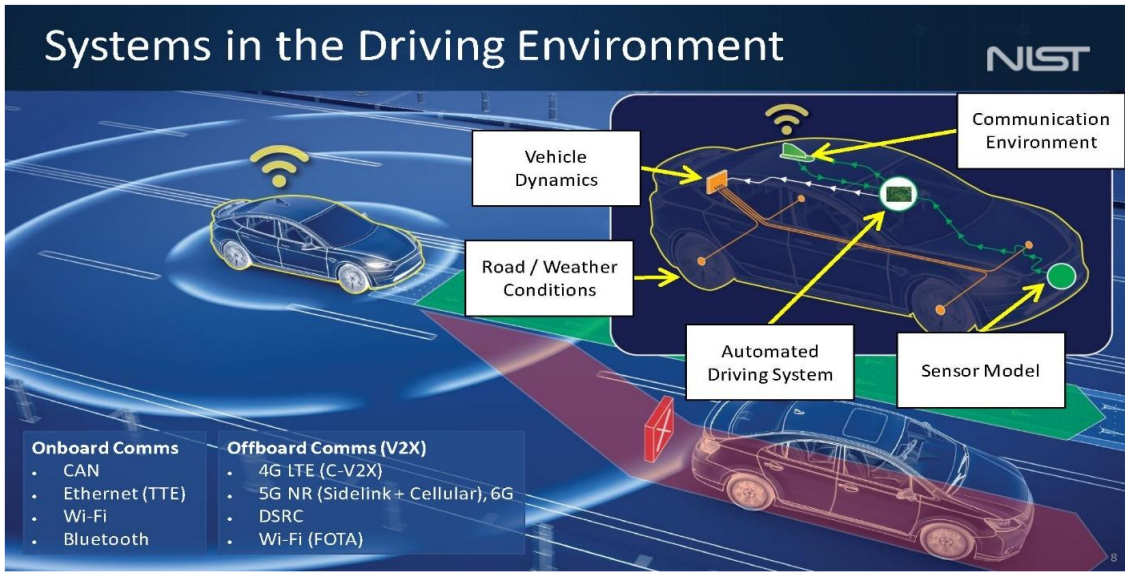

Fig. 2. Onboard and offboard connections in AVs.

The AV community envisions several different V2X application types and use cases, such as vehicle platooning, advanced driving, extended sensors, remote and cooperative driving, and vehicle quality of service support.

Communications pathways between systems are complex and could be subject to various forms of interference in the driving environment that can affect overall vehicle performance (Fig. 2). Advanced reliable communications and security features will be important as these networks evolve. Direct links, side links, and cellular networks should be integrated to provide the level of service needed. Important features include spectrum flexibility, sensing, scheduling feedback-based transmission, and quality of service (QoS). NIST is currently exploring a number of AV use case scenarios related to security, privacy, vehicle response to collision risks, the integration of AV systems, and the co-simulation of network responses (e.g., data transfer, time/latency, etc).

The AV community envisions several different V2X application types and use cases, such as vehicle platooning, advanced driving, extended sensors, remote and cooperative driving, and vehicle quality of service support.

6.3. Feedback on Current Programs and Activities

NIST's work on AV communications is considered impactful and helpful to the AV community. There are several organizations that could be important collaborators on AV com-

munications as technology moves forward, including SDOs, government agencies, and telecommunications companies.

Standardization was a key topic, and recommendations were made to explore various communication protocols and modes (e.g., V2X, V2N, etc), particularly protocols for authentication and trust. Other areas for potential investigation included best practices relative to vehicle performance and features from the owner-operator perspective (e.g., likelihood of communication failures and responses). Another area of interest was testing and benchmarking, which could support best practice protocols. Data compression, speed, security, and accuracy in AV communications were noted as possible topics of interest.

Table 18 (from Appendix F) provides a summary of these communications comments and suggestions.

6.4. Identification of Challenges

AV communications face many potential challenges, including latency requirements, infrastructure availability, lack of spectrum, and slow government mandates that could catalyze the development of consistent communication protocols. Standardizing interactions with other AV systems should be accelerated, and organizations involved with AV standards (e.g., SAE, 3GPP, IEEE, and others) should coordinate on and contribute to standardization activities. Differences and gaps across international standards for AVs also need to be considered and resolved.

The integration of AV communications with external infrastructure was seen as a broad challenge for the future. There is a lack of functionality and consistency in how technologies will be deployed among different regions, and available spectrum and cooperative localization are immediate issues. Competing uses for cellular networks for non-critical communications could lead to traffic management issues. Managing signal interference, overlaps, latency, and potential blind spots (i.e., data dead zones) could also impact the reliability of communications.

Table 19 (from Appendix F) summarizes some of the challenges that stakeholders identified as limiting AV communications progress and standardization.

6.5. Approaches and Needs for Research and Testing

There are many different approaches for researching and testing AV communication systems for effectiveness, such as simulation, physical measurement-based testing, or some combination of these. Hybrid approaches with mixed communications may be the most reasonable approach. The types of scenarios to be studied primarily include those that will ensure the safety and reliability of the vehicle in operation. It could be important to establish advanced mobility regions across the country where prototypes could be deployed and scenarios evaluated under real-world conditions.

Some important scenarios for testing could include mean time to respond and related metrics, intersection scenarios (e.g., occluded or blind spots), harsh weather conditions, unique infrastructure (e.g., tunnels, urban canyons, etc), system optimization and robustness under difficult driving conditions, and overall system reliability for safety.

Simulations were recommended as the most important alternative to physical testing considering the enormous number of scenarios, actors, and situations that arise. Simulation could be used to eliminate some options, followed by physical testing to advance the most promising options under real-world conditions that affect performance (i.e., hybrid of simulation and physical testing). QoS, security, and latency testing were noted as some of the most important elements for testing.

Table 20 (from Appendix F) summarizes the proposed areas and approaches for researching and testing AV communications and key scenarios.

7. Artificial Intelligence

7.1. Industry Keynote Overview

Aleksander Madry, Director of the Center for Deployable Machine Learning, MIT, and Research Staff at OpenAI — Robust ML: Where Are We?

Aleksander Madry highlighted the most critical failure modes of ML that should be addressed with more robustness: adversarial, data poisoning, and distribution shift brittleness. One potential solution is to identify consistent failure modes for each in a systematic way. This would require making ML more robust, which in turn requires an understanding and control of how the data factors into model decisions. New paradigms are needed that provide robustness for ML systems by identifying cognitive problems and devising solutions and interventions that are effective and safe. For example, one approach is to revise how signals and concepts are processed by the model to enable better ML outcomes (Fig. 3).

Aleksander Madry also discussed the importance of considering scene variation and related impacts on AI robustness, testing the competency of AI systems and tools, and conducting test cases for validation.

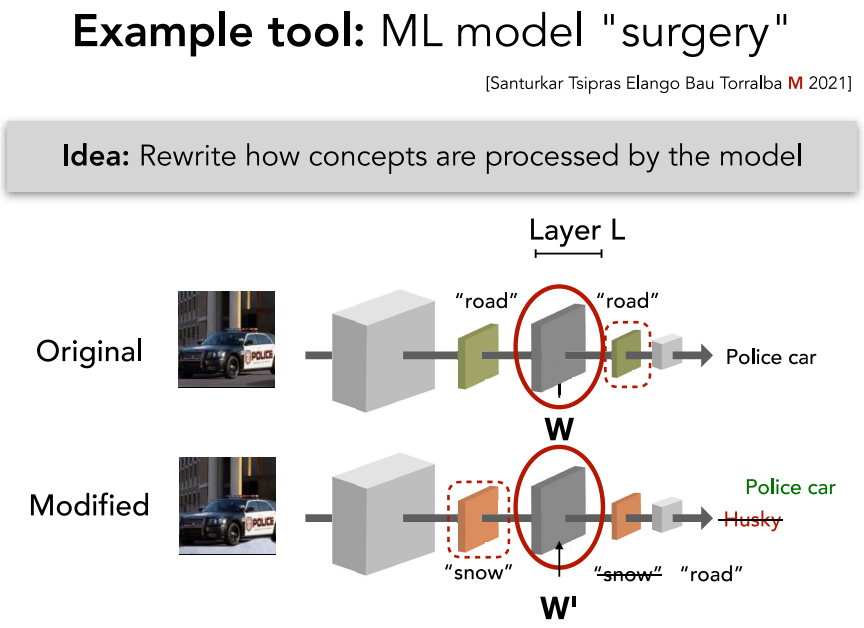

Fig. 3. New approaches for more robust machine learning in AVs (slide from Aleksander Madry's presentation).

7.2. Scope

This workshop was part of NIST's ongoing efforts to connect with stakeholders from industry, government, and academia to collaborate on ideas regarding AI models for ADS. AI plays a pivotal role in enabling vehicles to navigate and operate on their own. For example, perception AI is critical for ADS to process data from various sensors to interpret and understand the vehicle's surroundings. ML models are trained to recognize and classify objects, pedestrians, road signs, lane markings, and other relevant information in real time. If these models are not robust, the omission or misclassification of road objects can lead to crashes or near misses, and the current ADS safety record is lagging behind human driver performance for the same number of traveled miles. Therefore, it is necessary to develop improved mechanisms for the technical evaluation of object detection and classification in AI perception systems.

NIST currently has a graphics processing unit (GPU) cluster with open-source models and public datasets and has procured an automated test vehicle to validate initial AI test methods. NIST has also developed Dioptra (https://pages.nist.gov/dioptra/), a ML security testbed. Dioptra provides a modular framework for running, tracking, and organizing ex-

periments that test the robustness of ML models against various types of adversarial attacks.

NIST AI 100-2[5] describes a taxonomy of attacks and mitigations and defines terminology in the field of adversarial machine learning (AML). This report can be used in conjunction with the Artificial Intelligence Risk Management Framework (NIST AI RMF 100-1)[6] to identify and mitigate risks in AV applications. While there are many types of ML attacks, NIST AI 100-2 identifies three categories that can be applied to AVs: evasion, poisoning, and privacy. In evasion attacks, an adversary manipulates the test data that results in poor AV performance. Poisoning attacks alter the training data used to create or maintain a model with the intention of causing it to learn incorrect associations, such as with image detection algorithms. Privacy attacks attempt to "reverse engineer" an ML model. By tailoring Dioptra for the AV community, stakeholders will be prepared for AV attacks that influence uncertainty. Specific requirements to support standards and manage risk for AI use are needed, such as the data description object (DDO) format and a data interrogation sheet (DIS) to manage uncertainty and risk in AVs. By extending NIST's AI Risk Management Framework, NIST has drafted a DDO format and a DIS. Simulations and ML models can be appropriately described for evaluation with a standardized DDO format, and external stakeholders can use the DIS to access the DDO format.

This discussion session focused on:

- Gaining feedback on current NIST research and testbed activities
- Understanding current and future measurement, testing, and standardization challenges to the reliable use of AI in automated driving systems.
- Identifying approaches and needs for future R&D and testing.

The results of these discussions are summarized in the following sections.

7.3. Feedback on Current Programs and Activities

Overall feedback emphasized the importance of communication and collaboration within the realm of AVs. NIST was noted as playing a pivotal role in bringing together diverse stakeholders from conventional automotive companies, academia, and government agencies to facilitate knowledge exchange and cross-industry dialogue. Streamlining communication across these different sectors will require standardized language, as well as public resource and dataset sharing to support research and uncertainty metric evaluation, even in cases where organizations might be hesitant to share. This emphasis on improved communication and collaboration was a prevailing theme that emerged across all of the AI workshop discussions.

[5] The 2023 edition of this report is available at https://csrc.nist.gov/pubs/ai/100/2/e2023/final.
[6] This report is available https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

Table 21 (from Appendix G) provides a summary of comments and proposed improvements and recommendations for NIST activities.

7.4. Identification of Challenges

A number of challenges were identified that impact the ability to use AI technologies to improve object detection and classification in AVs, such as the robust identification of corner/edge scenarios, computational constraints, changing environmental conditions, sensor fusion and communication complexities, and the need for comprehensive and diverse datasets. These challenges underscore the multifaceted nature of achieving fully autonomous vehicles with AI and emphasize the importance of innovative solutions and cross-industry collaboration to overcome them.

Identifying real-world corner/edge cases is challenging as there are potentially an infinite number (e.g., children at play, workers performing various tasks, emergency responders, etc). Regardless, such scenarios can have dire consequences and an effective methodology for identifying and addressing them is lacking.

While sensor combinations and fusion could enhance safety, there are still uncertainties about how well the vehicle will make decisions based on collective data from a variety of sources. For example, AI may not have the ability to recognize every nuance and perform effectively depending on weather conditions, electromagnetic interference, light versus darkness, or road changes.

Table 22 (from Appendix G) fully summarizes the challenges discussed.

7.5. Approaches and Needs for Research and Testing

Several major topics for research and testing will be important for future AI and ML systems, including harnessing real-world data, fostering collaboration between AI and transportation standards groups, and using ensemble methods. For example, there is a wealth of untapped data from DOT-supported Transportation Operation Centers that receive data streams and camera feeds. This data could be transformed into training sets and system models for object recognition. Data obtained in controlled test settings could also be utilized for training, such as data from depleted or unusual environments (e.g., rain, fog, partial obstructions, etc).

Many suggestions for standardization emerged, including standardized competency tests, open-source code for testing, and establishing metrics for safety evaluation and object classification taxonomy. Open-source code could be leveraged to develop testing methods for evaluating model performance in specific scenarios and conditions, which could then be standardized for best practices.

These ideas emphasized the importance of outreach and collaboration among SDOs and other organizations to accelerate the deployment of AI technologies for AVs. These ef-

forts could include groups such as ISO joint technical committee (JTC) and SAE committees, where expertise and prior standards efforts in the areas would help to promote information exchange and collaboration on future standards. Communities of interest could also be helpful in identifying and designing specific road scenarios for benchmarking and road tests.

Table 23 (from Appendix G) summarizes the common themes for approaches to characterize, validate, and standardize testing for AI.

8. Infrastructure

8.1. Session Keynote Overview

The session keynote is formatted as a fireside chat featuring Ed Staub, VP and Director of the Automation Office at SAE, and Kelley Coyner from Leidos. The conversation revolves around the evolving relationship between physical and digital infrastructure and AVs. A summary of the discussion is provided below.

The speakers discuss the historical and current contributions of SAE in setting standards that accommodate the shift towards automation in vehicles. This includes the establishment of cooperative driving automation committees and their focus on various aspects of AV integration such as prescriptive cooperation and vehicle communication protocols.

There is an emphasis on the importance of both physical (e.g., road markings, signage) and digital infrastructure (e.g., connectivity, data communication) to support AV deployment and operation. The dialogue addresses how inconsistencies in infrastructure can hinder AV functionality and safety.

The discussion includes how AV technology and infrastructure need to co-evolve. The integration of vehicle technology with road infrastructure is critical for the localization and operation of AVs, enhancing safety and operational efficiency.

Several challenges are mentioned, such as the variability of infrastructure across jurisdictions and the potential delay in AV deployment due to the slow implementation of necessary digital infrastructure. The conversation also touches on the ”contentious” nature of relying on digital messages for AV operations and the need for standardization.

The speakers propose focusing on standardizing digital infrastructure to improve consistency and reliability for AVs. There is also a call for more research and pilot projects to explore the effective deployment of AVs in varied infrastructural settings.

8.2. Industry Keynote Overview

Jeffrey Wishart, Fellow at the Science Foundation of Arizona — Digital Infrastructure Research in AZ

Dr. Wishart discussed the Arizona Commerce Authority's Institute of Automated Mobility (IAM), which has been researching digital infrastructure and how it can be used to improve intersection safety through their SMARTDRIVE testbed at a number of intersections in Anthem, AZ. The testbed collects data from infrastructure-, drone-, and ground-based cameras; differential GPS; and infrastructure-based LiDAR (Fig. 4). The system uses a camera-based detection and tracking algorithm to capture a defined set of driving assessment metrics, such as collision incidents, lane stability violations, and traffic law violations established by SAE J 3237[7]. These metrics can be used to evaluate human- and ADS-driven vehicles.

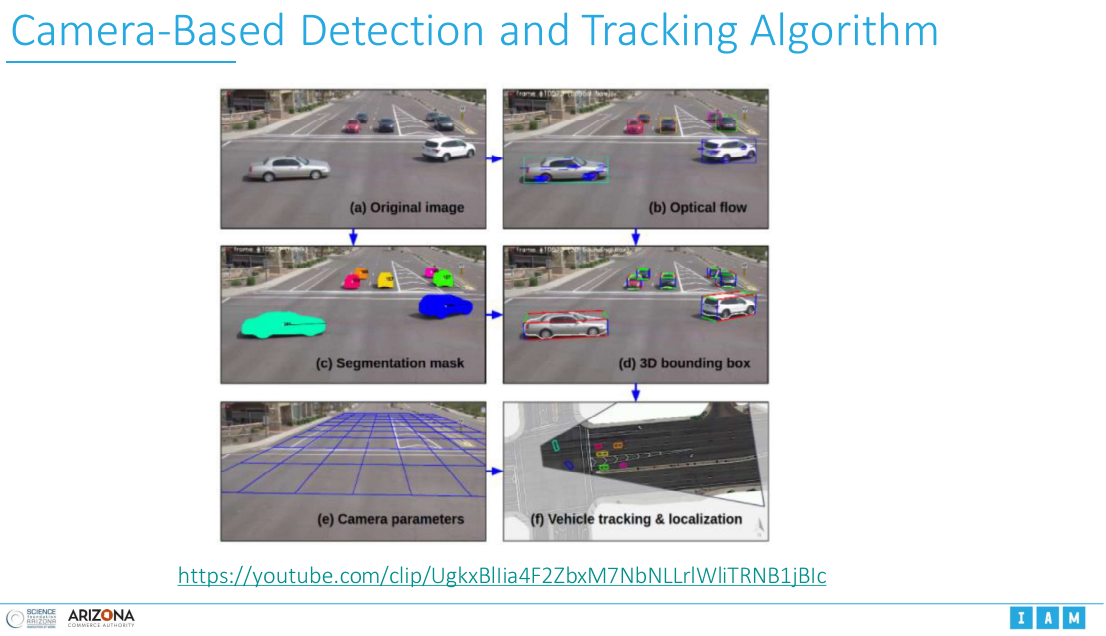

Fig. 4. IAM camera-based detection and tracking algorithm (slide from Jeffrey Wishart's presentation).

The IAM is currently identifying additional, prioritized locations for future digital infrastructure based on a number of criteria, including camera availability, automated vehicle testing

[7] https://www.sae.org/standards/content/j3237/

presence, and collision and traffic volumes. As many as 3,000 potential lighted intersections across Arizona are being considered. Other issues to be explored include intersection data collection, such as sensor modalities, detection and tracking algorithms, occlusions and shapes, and sensor movement. Next steps include applying to ARPA-I's Intersection Safety Challenge and the U.S. Department of Transportation (USDOT) SMART grant.

Michael Mollenhauer, Director of Technology Implementation at the Virginia Tech Transportation Institute — Connected and Automated Vehicle Projects

Dr. Mollenhauer directs activities at the Virginia Tech Transportation Institute (VTTI), leading over 300 active projects and collaborating with over 100 sponsors across the private and public sectors. Vulnerable road user (VRU)'s research has positively influenced public policies for driver, passenger, and pedestrian safety and reduced the environmental impacts of transportation. Dr. Mollenhauer also shared information about the Virginia Connected Corridors (VCC) program, which covers major traffic corridors in Virginia (Fig. 5) to facilitate the real-world development and deployment of connected-vehicle technology through roadside equipment, on-board technology, a developer-friendly cloud computing environment, and data exchange services.

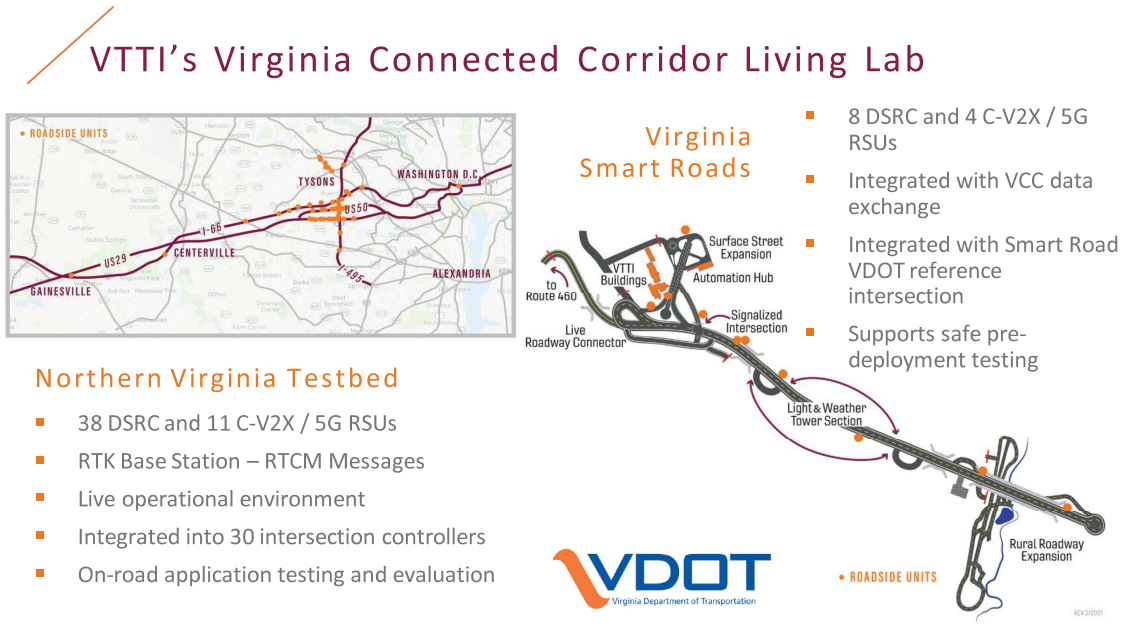

Fig. 5. Virginia Tech Connected Corridor Living Lab (slide from Michael Mollenhauer's presentation).

Dr. Mollenhauer highlighted one of the first C-V2X deployments on U.S. infrastructure that provides participating drivers with advisories on work zones and traffic control statuses. In addition, the Virginia DOT (VDOT) plans to deploy four smart intersection technologies in a pilot program that will help guide recommendations for future VDOT deployments and accelerate value recognition in early connected vehicles (CVs). VTTI is also working on a CV fleet management concept and safety monitoring for a low-speed automated shuttle in Fairfax County. These programs are important steps in the deployment and adoption of automated vehicles.

Henry Liu, Director of the Center for Connected & Automated Transportation (CCAT) — Smart Intersections and Ann Arbor Connected Environment 2.0 (AACE)

Dr. Liu is a Professor of Civil and Environmental Engineering at the University of Michigan, Ann Arbor and directs activities at the Center for Connected & Automated Transportation (CCAT), which is one of the USDOT's University Transportation Centers. Dr. Liu shared in-

formation on the University of Michigan's connected vehicle research programs, which began with the Safety Pilot Model Deployment (SPMD) in 2012, the world's first large-scale deployment of CVs in active infrastructure. Today, the Smart Intersection Project (SIP) builds on SPMD's foundation by developing an infrastructure-assisted cooperative driving automation testbed to accelerate CAV deployment and build a roadmap for its commercialization. SIP uses dynamic traffic signal control systems, roadside C-V2X units, and infrastructure sensors to communicate with connected vehicles and manages all of this data from centralized cloud-connected servers.

In addition to SIP, the University of Michigan manages Ann Arbor Connected Environment 2.0 (AACE 2.0), a program that aims to convert existing CV deployment to C-V2X by implementing the 5G Automotive Association (5GAA) Day-1 Applications. This program has been implemented at dozens of sites across Ann Arbor, including a dangerous roundabout intersection that had 69 crashes in 2020. AACE 2.0 deploys GRIDSMART cameras and roadside edge computers equipped with a robust perception model that communicates to cloud servers and third-party conflict/crash detection algorithms. This provides valuable data to inform crash prevention solutions. This infrastructure could also provide safety statistics on future CAVs.

A complete list of USDOT-supported University Transportation Centers and more information about each can be found at https://www.transportation.gov/research-and-technology/utcs-and-connected-vehicles.

Craig Hinners, Intelligent Transportation Systems (ITS) Solutions Architect at NoTraffic — State of the Practice for Connected Intersections

Mr. Hinners spoke about NoTraffic's work on intelligent transportation systems (ITS) to digitize the foundation of transportation, improve safety and traffic efficiency, and reduce CO2 emissions. He spoke on the current state of the connected intersections space, beginning with the three models for V2X data exchange: direct (V2I), edge (incorporating a field computer), and cloud. There have been two major developments in the connected vehicles space. First, the Federal Communications Commission (FCC) has granted a waiver for C-V2X technology to be used in the 5.9 GHz band. Second, ITS America published the National V2X Deployment Plan[8] in April 2023.

Future smart traffic detection systems will provide more information about vehicles and key roadway safety information than existing systems, such as vehicles in front and behind, pedestrians, traffic obstacles, and oncoming traffic. This will require reliable C-V2X infrastructure systems. CV infrastructure deployment may occur across multiple timescales — starting with emergency vehicles, public transportation vehicles, and fleet vehicles in the near-term and comprehensive systems that include data from all passenger vehicles, bikers, and pedestrian traffic in the long-term. While current traffic detection systems mainly focus on traffic equity using simple sensors to optimize traffic flow, smart traffic detection

[8] https://itsa.org/advocacy-material/its-america-national-v2x-deployment-plan/

systems could provide far more data to cars and pedestrians to improve safety by alerting them to upcoming red lights, stopped traffic, and pedestrian/car conflicts to prevent accidents.

8.3. Scope

AVs will need updates on driving conditions and the ability to utilize an array of roadway infrastructure systems that collect, interpret, and transmit signals to AVs on vital elements, such as traffic, construction, and road conditions. Studies have noted that roadside infrastructure could transmit updates on road conditions using beams of concentrated, millimeter radio waves. Other systems will need to interact with the vehicle to ensure safety. V2X technology will also be critical to communications between a vehicle and other vehicles, infrastructure, and pedestrians.

NIST is exploring collaborations with national standards organizations to develop a use-case template to drive a community-wide collection/definition of use cases and proven solutions across the U.S. Some basic engineering support will be required to accelerate the development and implementation of solutions for use cases. In particular, the operational capabilities and characteristics of available technology need to be measured and published so that developers and implementers know which particular technology instantiations they should deploy. It was proposed that NIST collect such data and work with the aforementioned national standards organizations to publish it.

8.4. AVs and Digital Infrastructure — Discussion Session

A number of questions were posed around the important components of digital infrastructure, obstacles to deployment, safety considerations, and infrastructure-AV relationships. The discussions around these questions are summarized in the following sections.

8.4.1. Digital Infrastructure Defined

Some of the key components of digital infrastructure relevant to AV implementation include situational awareness, communications/connectivity, ML, and AI. Relationships between AVs and a variety of infrastructure elements will need to be defined and evaluated for AV deployments to be successful nationally. Several elements of digital infrastructure were identified as important for holistic evaluation (Table 1).

One approach for handling these competing yet interconnected elements is a system-level analysis using robust curated models. This would incorporate technology for system-of-systems level co-simulation (drawing on prior work, such as the Universal CPS Environment for Federation (UCEF) [6]), and guidelines for how interconnected issues should be considered.

The Federal Highway Administration (FHWA) considers local traffic laws to be part of digital infrastructure, which increases the complexity of these digital relationships. The U.S. and Canada are two of the only countries in the world without national traffic laws that apply across states and provinces. As a result, there are thousands of different agencies at the state, county, and city levels writing and enforcing traffic laws. Scaling AVs nationally will require machine-understandable versions of all the relevant traffic laws.

Table 1. Key Elements of Digital Infrastructure Relevant to AVs.

Category	Elements
Common Vehicle-to-Infrastructure Elements	• Road traffic. • Sensing and control. • Cyber communication. • Operational workflows at the traffic control center involving decision making about traffic management (e.g., lane closures, diversions, speed limit changes). • Other AVs. • V2X communication and control.
Grid Infrastructure	• Impact on the electric grid as more EVs use different charging stations depending on traffic flows.
External Interactions	• Public transit. • Pedestrian traffic. • Special events (e.g., football game, music concert).

8.4.2. Digital Infrastructure and Safety

There were a number of examples in which digital infrastructure could potentially increase roadway safety, such as VRU safety, human driver safety, and first responder support. Digital infrastructure could also serve to streamline infrastructure owner and operator (IOO) operations and simplify AV deployment. The perspectives generated during discussions on safety are shown in Table 2.

Digital infrastructure has the potential to significantly enhance roadway safety by leveraging technology to facilitate better communication, data analysis, and real-time responses to dynamic road conditions to the benefit of both AVs and VRUs. Communication with first responders will become easier, automated, and more efficient. Key metrics include reducing the number of safety-related incidences and improving the speed of response

when those incidents occur. New digital infrastructure must be optimally compatible with existing infrastructure to facilitate a smooth transition and interoperability.

Table 2. Digital Infrastructure Safety Elements for AVs.

Category	Digital Infrastructure Safety Elements
Security	• Stand-alone digital infrastructures to enable AVs to navigate to safe spots or homes even if the vehicle is offline. • Stringent cybersecurity measures to protect data and privacy and ensure the safe operation of the digital infrastructure.
Vulnerable Road User (VRU) Safety	• Infrastructure with systems to detect pedestrians and other vulnerable road users and alert vehicles to their presence • Integration of crosswalk signals with vehicle systems to ensure that vehicles stop for pedestrians at crosswalks.
Training	• Training programs to educate road users and stakeholders on the safe use of the digital infrastructure.
Human Driver Safety	• ADASs to help human drivers make safe decisions (e.g., lane-keeping assistance, automatic emergency braking). • Real-time alerts and updates on traffic conditions to help drivers avoid accidents and congestion.
First Responders	• Priority lane assignments and traffic light preemption to facilitate the rapid response of emergency services. • Real-time reporting of incidents to first responders through connected systems.

Streamlining IOO Operations	• Use of data analytics to perform predictive maintenance, reduce sudden breakdowns, and enhance safety. • Implementation of intelligent smart traffic management systems to control traffic flow and reduce congestion.
AV Deployment	• Standardized communication protocols to facilitate seamless interactions between AVs and infrastructure. • High-definition maps integrated with real-time updates to enable AVs to navigate safely and efficiently.
Collaborative Planning and Technology Adoption	• Engagement with stakeholders (e.g., government agencies, industry players, the community) throughout the planning process to ensure that the infrastructure meets the needs of all road users. • Phased adoption of new technologies to allow for testing and refinement before wide-scale implementation.

8.4.3. Digital Infrastructure and AV Deployment

Well-equipped digital infrastructure can support an effective nationwide deployment of AVs. For example, infrastructure can provide situational awareness, mitigate challenges faced by AVs, and potentially simplify ADS designs. Table 3 illustrates some of the perspectives on how digital infrastructure can accelerate the use of AVs.

Ensuring safety and operational efficiency should be the primary considerations for priority control over AVs (infrastructure versus vehicle), regardless of the strategy adopted. The AV should be able to switch between metropolitan and rural locations and scenarios, so a flexible approach to priority control that considers the specific characteristics of different environments could provide a balanced solution. A regulatory framework will also be needed to govern the control dynamics to ensure safe and efficient operation while avoiding potential conflicts and misuse.

Table 3. Capabilities to Accelerate AV Deployment.

Category	Acceleration Elements
Situational Awareness	• Broadcast basic safety messages (BSMs). • Real-time data, including BSM, to keep all vehicles updated with the latest road conditions and support cooperative collision avoidance.
AV Challenges	• Infrastructure-to-vehicle (I2V) communications to support AV navigation, especially in complex and dynamic environments. • Harmonized standards for AV operation to ensure seamless integration with various infrastructure elements and other vehicles.
Automated Driving Systems (ADS) Design	• Detailed real-time information from infrastructure elements to potentially reduce the sensor burden on AVs. • Ability to handle complex driving scenarios by leveraging infrastructure-based sensors and communications systems.
Priority Control Over AVs	• Considerations for safety, efficiency, and the operational dynamics of various environments to determine whether priority control should reside with the vehicle or the transportation infrastructure.

8.4.4. Obstacles to the Deployment of Digital Infrastructure

A number of infrastructure challenges will need to be addressed for effective V2I communication. For example, it is challenging to accurately determine the location of a rapidly moving AV and track it while simultaneously producing an optimum beam to reliably transmit data at high rates and low latency. Moreover, the costs of infrastructure development and deployment, continuous maintenance, and modernization as technology emerges and improves will be high. The diversity of stakeholders required to invest in this effort (e.g., federal, state, and local governments; communities; private companies; etc) increases complexity and the need for collaboration and coordination.

Fully integrating AVs into conventional roadways and communities will require policies and guidelines for infrastructure that are currently lacking, such as guidance infrastruc-

ture (e.g., line marking and signage), communication networks, parking, service stations, and construction zones. Infrastructure is needed that can be readily interpreted by AVs and provide real-time traffic and environmental information. Table 4 summarizes the obstacles identified. The categories are not based on any prioritization of topics but grouped for convenience and readability.

Table 4. Obstacles to the Deployment of Digital Infrastructure for AVs.

Category	Challenges and Obstacles
Economics	• High initial costs of developing a comprehensive digital infrastructure (i.e., a substantial investment in technology, hardware, and skilled personnel). • Significant continuing costs for ongoing maintenance and updates to the infrastructure.
Regulations and Policies	• Lack of regulations for digital infrastructure and AVs. • Lack of consensus for implementation priorities due to divergent perspectives, interests, and political dynamics.
Resources	• Limited funding for R&D and implementation as well as limited access to the results of these activities (e.g., US DOT budget for smart infrastructure is 1/30th that of China).
Intellectual Property and Knowledge Sharing	• Companies restricting access to research findings and technology development, which impedes collaborative efforts and slows down deployment and progress. • Lack of platforms through which researchers and developers can share findings and collaborate.
Standardization	• Lack of standards leading to issues of interoperability, safety, and security.

Pace of Development	• Rapid technological advances leading to infrastructure that quickly becomes outdated and requires frequent updates and upgrades.
Security	• Susceptibility to constantly evolving threat scenarios.

8.4.5. Enabling Digital Infrastructure

There were a number of suggestions for enabling the integration of digital infrastructure with AVs (see Table 5). These initiatives will involve collaboration, data compilation, and a coordinated national approach to infrastructure development. Existing regulatory frameworks will need to be revised to accommodate emerging digital technologies, and the transportation community could also take strategic steps to foster the development and integration of digital infrastructure.

Table 5. Actions to Enable the Deployment of Digital Infrastructure for AVs.

Category	Potential Actions
Traffic Laws and Regulations	• Work with AV developers to create a "digital twin" of U.S. traffic laws (preliminary examples in Japan)[9].

[9] See https://www.aichi-steel.co.jp/ENGLISH/smart/mi/gmps/.

National Infrastructure Use Case Databases	• Centralized Knowledge Repository: Various use cases to demonstrate scenarios in which digital infrastructure can be effectively deployed. • Benchmarking Database: Benchmark the performance of different technologies and strategies to aid stakeholders in making informed decisions. • Best Practices Solutions Database: Compile solutions that have proven effective to disseminate best practices, encourage their adoption across different regions, and enable stakeholders to learn from past experiences. • National Prioritization of Use Case Implementations: Establish national priorities for the most important use cases and solutions to coordinate the development of digital infrastructure and guide investments in critical and beneficial projects for optimum resource utilization.
Characterization of Digital Infrastructure Technology	• Program to characterize digital infrastructure technology: – Technology Assessment: A thorough assessment of various digital infrastructure technologies to better understand their capabilities and limitations. – Standardization: Characterization of technologies as a precursor to developing standards in order to promote interoperability and seamless integration.
Engaging with Industry Partners and Academia	• Collaborative R&D: Collaborative research and development initiatives with industry partners and academia to foster innovation and accelerate technology development. • Pilot Programs: Engagement with industry partners to launch pilot programs to test new technologies and solutions in real-world settings.

Education and Awareness	• Educational campaigns to inform the public about the benefits of digital infrastructure and gather feedback on their concerns and preferences. • Programs to develop necessary skill sets in the existing workforce to utilize new digital infrastructure technologies. • Transparent communication to build public trust in DI technologies.

8.4.6. Implementing Digital Infrastructure

Implementing digital infrastructure should involve collaborative planning, technology evaluation, stakeholder engagement, and phased deployment. Regulations and policy development, technology design and deployment, advances, and training on new technologies and systems will all be key components. The following pathways were also suggested:

8.4.6.1. Strategic Planning and Vision Setting

- Setting Clear Objectives: Define clear objectives that align with broader transportation and societal goals.
- Comprehensive Research: Conduct comprehensive research to understand the latest technological advancements and best practices globally.

8.4.6.2. Stakeholder Engagement and Collaboration

- Multi-Stakeholder Collaboration: Facilitate collaboration among government agencies, industry players, academia, and the community.
- Feedback and Input: Solicit feedback and input from all stakeholders to ensure that the infrastructure meets the diverse needs of the community.

8.4.6.3. Regulatory Framework and Policy Developments

- Regulatory Adjustments: Develop and adjust regulatory frameworks to foster innovation while also ensuring safety and privacy.
- Standardization: Standardize technologies and protocols to ensure interoperability and security.

8.4.6.4. Technology Evaluation and Selection

- Pilot Programs: Initiate pilot programs to test and evaluate different technologies in real-world settings before full-scale deployment.
- Performance Metrics: Develop performance metrics to objectively assess the effectiveness of different technologies.

8.4.6.5. Infrastructure Design and Development

- Modular Design: Adopt a modular design approach to allow for scalability and future upgrades.
- Resilient Infrastructure: Build resilient infrastructure that can withstand various challenges, including cybersecurity threats and environmental impacts.

8.4.6.6. Funding and Investment

- Sustainable Funding Models: Develop sustainable funding models to finance infrastructure development, including public-private partnerships.
- Grants and Incentives: Explore opportunities for grants and incentives to encourage investment in digital infrastructure.

8.4.6.7. Implementation and Deployment

- Phased Deployment: Implement the infrastructure in phases, starting with critical areas and gradually expanding to other regions.
- Integration With Existing Infrastructure: Ensure that the new infrastructure integrates seamlessly with existing infrastructure.

8.4.6.8. Training and Capacity Building

- Workforce Training: Develop training programs to build the workforce's capacity to utilize the new digital infrastructure.
- Community Education: Educate the community about the new infrastructure and how to use it safely and effectively.

8.4.6.9. Monitoring, Evaluation, and Continuous Improvement

- Real-Time Monitoring: Set up systems to monitor the infrastructure in real time and ensure optimal performance.

- Feedback Loops: Establish feedback loops to learn from past experiences, make necessary adjustments, and continuously improve.

8.4.6.10. Public Engagement and Awareness

- Public Awareness Campaigns: Launch public awareness campaigns to inform the public about the benefits of the new infrastructure and foster acceptance.
- Feedback and Suggestions:Encourage public feedback and suggestions to ensure that the infrastructure meets the needs and expectations of the community.

8.4.7. Relationship Between AVs and Digital Infrastructure

AVs are changing transportation, and a robust digital infrastructure will be central to ensuring efficiency, safety, and sustainability. Effective relationships should be guided by the principles of interoperability, real-time data exchange, and collaborative intelligence.

Emerging relationships between AVs and Digital Infrastructure (DI) should also be dynamic, collaborative, and adaptive to promote this vision of cooperative mobility. AVs should be capable of autonomous operation with minimal reliance on infrastructure and showcase adaptive functionalities to navigate diverse environments. Data sharing between OEMs and road owners should be encouraged and enabled, and the issues of liability and accuracy should be considered. Table 6 summarizes some of these relationships and important connections. The topics are not prioritized but are categorized for readability.

Table 6. Key Digital Infrastructure and AV Relationships.

Category	Key Areas of Connection
Data Exchange Mechanisms	• Encourage and enable the global sharing of key data on infrastructure relevant to AVs (e.g., ADAS sensors can detect degraded physical infrastructure). – Set up an organization to guarantee data anonymity (similar to the Automotive Information Sharing and Analysis Center (Auto-ISAC)) and ensure that it gets to appropriate road owners. – Standardize ways to share information without violating privacy.

Interconnected Ecosystems	• Establish an interconnected ecosystem where AVs seamlessly communicate with each other and with infrastructure. – Standardize communication protocols that facilitate the real-time exchange of vital information, such as traffic conditions, weather updates, and road obstructions. – Harmonize environments in which data from diverse sensors and sources converge, and provide a comprehensive overview of the transportation landscape to aid AV navigation and decision-making.
Adaptive and Predictive Algorithms	• Incorporate adaptive and predictive algorithms that utilize ML and AI to continuously learn and evolve based on real-time data, and enable AVs to make informed decisions, especially in complex driving scenarios.
Dynamic Traffic Management	• Develop a traffic management system in which traffic signals, lane allocations, and speed limits are dynamically adjusted based on real-time traffic conditions to optimize flow and minimize congestion, and equip AVs with systems to effectively interpret and respond to these dynamic signals.
Cybersecurity and Data Privacy	• Prioritize infrastructure cybersecurity and data privacy through the development of secure platforms with embedded features to protect against cyber attacks and unauthorized data access, and require that AVs adhere to cybersecurity norms.
Rural and Urban Disparities	• Acknowledge and address disparities between rural and urban settings (e.g., urban environments may benefit from highly interconnected digital infrastructure, while rural settings might pose challenges in terms of connectivity and sensor deployments).

Cooperative Collision Avoidance	• Foster cooperative collision avoidance systems that integrate inputs from roadside sensors, vehicular sensors, and pedestrian devices. – Incorporate the dynamic interplay of V2X communications to develop a synchronized and responsive transportation grid (i.e., proactive AV responses to avoid accidents).

8.4.8. Control Relationships

There were discussions about how digital infrastructure should be designed and controlled, the differences between rural and metropolitan environments, and the dynamic nature of those relationships, which often depend on situations that occur locally. For example, changing between metropolitan and rural environments may involve different types of climates (e.g., very dry versus wet, severe, or normal, etc). If the transportation infrastructure maintains priority control over AVs, a dynamic and interconnected network of systems could be developed to help control traffic flow, reduce congestion, and enhance safety. This would take advantage of centralized control mechanisms, including AI algorithms that process real-time data. Conversely, priority control within the vehicle would result in a decentralized system in which each AV makes decisions based on its onboard sensors and computing capabilities. Vehicles would employ V2V communication to share information and autonomously negotiate movements.

Applying these conceptual frameworks to the different characteristics of metropolitan and rural settings will require a customized, flexible strategy that dynamically shifts priority control between infrastructure and vehicles based on the demands of the environment. Table 7 summarizes these perspectives.

Table 7. Control Relationship Scenarios for DI and AVs.

Category	Relationships
Infrastructure-Led Control	• Benefits: – Centralized Decision-Making: A coordinated approach to traffic management that leverages global traffic data to make informed decisions. – Preventive Safety Measures: Use of predictive analytics to identify potential collision scenarios and take preventive measures. • Disadvantages: – Single Point of Failure: Can be a single point of failure, which poses significant risk in cases of system malfunction or cyber attacks. – High Infrastructural Investment: Substantial investment needed to develop and maintain a comprehensive digital infrastructure.
Vehicle Priority Control	• Benefits: – Decentralized Resilience: No single point of failure, which offers resilience against systemic breakdowns. – Scalability: Scales more easily and allows for the gradual introduction of AVs into the existing infrastructure. • Disadvantages: – Localized Decision-Making: Decisions based on limited, localized data, which potentially misses the broader context that infrastructure could provide. – Inter-Vehicle Coordination Challenges: : Coordinating maneuvers autonomously amongst a fleet of AVs can be complex, particularly in high-density traffic scenarios.

Urban vs. Rural Environments Control	• Metropolitan Environments: – Hybrid Approach: Infrastructure-led systems complement vehicle-centric control to ensure a high level of coordination while retaining individual vehicle autonomy for resilience. • Rural Environments: – Vehicle-Centric Control: AVs may safely and efficiently navigate with minimal infrastructure support in rural areas with lower traffic densities and simpler traffic scenarios. – Vehicle-Priority: Giving priority control to individual AVs might allow for more flexible and adaptive responses to changing road conditions. • Hybrid Environments: – Dynamic Hybrid Priority Assignment: A hybrid approach in which priority control can dynamically shift between the infrastructure and the vehicle based on the specific circumstances and the prevailing road conditions.

9. Path Forward

NIST has a long history of contributing to the development of AVs and is entering the final year of internal Strategic and Emerging Research Initiatives (SERI) funding for this program. The NIST SERI program is designed to fund high-impact, cross-disciplinary research projects that address critical national needs and emerging technological challenges. Stakeholders have emphasized the need for an enduring NIST presence in this space. There were many helpful and specific suggestions provided during the workshop that will be considered as the projects evolve. NIST is continuing to develop the methodology for systems interaction testing and testbed capabilities.

References

[1] Schlenoff C, Lightman S, Nguyen V, Rachakonda P, Zhang T, Aboul-Enein O, Barbosa N, Miller C, Sawyer D, Virts A (2022) Workshop report: Standards and performance metrics for on-road autonomous vehicles (National Institute of Standards and Technology, 100 Bureau, Dr. Gaithersburg, MD. USA), NIST IR 8442. https://doi.org/https://doi.org/10.6028/NIST.IR.8442

[2] RFI (2023) Request for Information on Implementation of the United States Government National Standards Strategy for Critical and Emerging Technology (USG NSSCET). Available at https://www.federalregister.gov/documents/2023/09/07/2023-19245/request-for-information-on-implementation-of-the-united-states-government-national-standards.

[3] ISO 26262-1:2018 - Road vehicles – Functional safety – Part 1: Vocabulary, https://www.iso.org/standard/68383.html.

[4] ISO 21448:2022 - Road vehicles – Safety of the intended functionality, https://www.iso.org/standard/77490.html.

[5] UNECE R156 - UN Regulation No. 156 – Software update and software update management system, https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update.

[6] Burns M, Roth T, Griffor E, Boynton P, Sztipanovits J, Neema H (2018) Universal CPS Environment for Federation (UCEF). *2018 Winter Simulation Innovation Workshop*. Available at https://api.semanticscholar.org/CorpusID:149679555.

Appendix A. Agenda

Day 1 – September 5, 2023		
Start	**End**	**Session: Systems Interaction**
10:30 am	10:45 am	Opening Remarks
10:45 am	10:50 am	Welcoming Remarks Congresswoman Haley Stevens
10:50 am	11:00 am	Welcoming Remarks Hannah Brown (NIST Deputy Associate Director of Laboratory Programs)
11:00 am	11:15 am	National Standard Strategy Presentation Jayne Morrow (NIST Senior Advisor for Standards Policy)
11:15 am	11:45 am	Overall Keynote Ann E. Carlson (Acting Administrator, NHTSA)
11:45 am	12:00 pm	Discussion of Output of Last Workshop
12:00 pm	12:30 pm	Systems Interaction Keynote David Agnew (Director, Dataspeed Inc.)
12:30 pm	1:00 pm	NIST Systems Interaction AV Effort Discussion
1:00 pm	1:15 pm	Break/Transition to Breakout Rooms
1:15 pm	2:30 pm	Systems Interaction Effort Breakout Discussion
2:30 pm	3:00 pm	Systems Interaction Effort Breakout Report
3:00 pm	4:00 pm	Workshop Adjourns for the Day
		Optional National Standards Strategy Discussion

Day 2 – September 6, 2023		
Start	**End**	**Session: Perception and Cybersecurity**
10:30 am	10:45 am	Opening Remarks
10:45 am	11:15 am	Perception Keynote Speech Rajeev Thakur (SAE Instructor for LiDAR and Infrared Camera Technologies)
11:15 am	11:45 am	NIST Perception AV Effort Discussion
11:45 am	12:00 pm	Break/Transition to Breakout Rooms
12:00 pm	1:15 pm	Perception Effort Breakout Discussion
1:15 pm	1:50 pm	Perception Effort Breakout Report
1:50 pm	2:20 pm	Cybersecurity Keynote Speech Anuja Sonalker (CEO and Co-Founder of STEER)
2:20 pm	2:50 pm	NIST Cybersecurity AV Effort Panel Discussion
2:50 pm	3:05 pm	Break/Transition to Breakout Rooms

3:05 pm	4:20 pm	Cybersecurity Effort Breakout Discussion
4:20 pm	5:00 pm	Cybersecurity Effort Breakout Report

Day 3 – September 7, 2023

Start	**End**	**Session: Communications and AI**
10:30 am	10:45 am	Opening Remarks
10:45 am	11:15 am	Communications Keynote Speech Jim Misener (Global V2X Ecosystem Lead, Qualcomm)
11:15 am	11:45 am	NIST Communications AV Effort Discussion
11:45 am	12:00 pm	Break/Transition to Breakout Rooms
12:00 pm	1:15 pm	Communications Effort Breakout Discussion
1:15 pm	1:50 pm	Communications Effort Breakout Report
1:50 pm	2:20 pm	AI Keynote Speech Aleksander Madry (Director of the Center for Deployable Machine Learning, MIT, and research staff at OpenAI)
2:20 pm	2:50 pm	NIST AI AV Effort Discussion
2:50 pm	3:05 pm	Break/Transition to Breakout Rooms
3:05 pm	4:20 pm	AI Effort Breakout Discussion
4:20 pm	5:00 pm	AI Effort Breakout Report

Day 4 – September 8, 2023

Start	**End**	**Session: Digital Infrastructure**
11:00 am	11:10 am	Welcome Ed Griffor, Marisa Walker
11:10 am	12:00 pm	Keynote: Fireside Chat with Ed Straub and Kelley Coyner Infrastructure Enablers and Transportation Automation
		Infrastructure Perspectives (Marisa Walker)
	10 min	Flash presentation 1 Jeff Wishart (SFAZ/ACA)
	10 min	Flash presentation 3 Mike Mollenhauer (VRU)
	10 min	Flash presentation 4 Henry Liu (M-City)
	10 min	Flash presentation 6 Craig Hinner's (NOTRAFFIC)
1:00 pm	1:10 pm	Break
1:10 pm	2:25 pm	Session Leader Team: G. Leeming/M. Dunaway

		Compiling a database of Infrastructure-Based, Safety-Critical Use Cases and Solutions
2:25 pm	2:40 pm	Session Leader Team: E. Griffor/C. Miller The NIST Role

Appendix B. List of Symbols, Abbreviations, and Acronyms

3GPP 3rd Generation Partnership Project.

5GAA 5G Automotive Association.

A-PNT Assured Positioning, Navigation, and Timing.

AACE Ann Arbor Connected Environment.

ADS Automated Driving System.

ADS TWG Automated Driving Systems Technical Working Group.

ADAS Advanced driver-assistance systems.

ADSIE Automated Driving Systems Interaction.

AEB Automatic emergency braking.

AI Artificial intelligence.

AML Adversarial machine learning.

API Application programming interface.

ASIL Automotive Safety Integrity Level.

Auto-ISAC Automotive Information Sharing and Analysis Center.

AV Automated Vehicle.

AV STEP ADS-equipped Vehicle Safety, Transparency and Evaluation Program.

AV TEST Automated Vehicle Transparency and Engagement for Safe Testing Initiative.

BOM Bill of materials.

BSM Basic safety message.

C-V2X Cellular-vehicle-to-everything.

CAMP Crash Avoidance Metrics Partners.

CAV Connected and automated vehicle.

CCAT Center for Connected & Automated Transportation.

CMM Coordinate Measuring Machine.

COI Community of interest.

CSRC Computer Security Resource Center.

CV Connected vehicle.

DDO Data description object.

DI Digital Infrastructure.

DIS Data interrogation sheet.

DOD Department of Defense.

DSRC Dedicated Short-Range Communications.

EEBL Emergency Electronic Brake Lights.

EMF Electromagnetic interference.

FCC Federal Communications Commission.

FHWA Federal Highway Administration.

GAN Generative adversarial network.

GPS Global Positioning System.

GPU Graphics processing unit.

I2V Infrastructure-to-vehicle.

IAM Institute of Automated Mobility.

ICS Industrial control system.

IMU Inertial measurement unit.

IOO Infrastructure owner and operator.

IoT Internet of Things.

ISO Organization for Standardization.

ITS Intelligent Transportation Systems.

ITSA Intelligent Transportation Society of America.

IVN In-vehicle network.

JTC Joint technical committee.

LED Light-emitting diode.

LiDAR Light Detection and Ranging.

ML Machine learning.

MTTR Mean time to remediate.

MUCTD Manual on Uniform Traffic Control Devices for Streets and Highways.

NCAP New Car Assessment Program.

NCCoE NIST National Cybersecurity Center of Excellence.

NGO Non-Governmental Organization.

NHTSA National Highway Traffic Safety Administration.

NIST National Institute of Standards and Technology.

NR New Radio.

ns-3 A discrete-event network simulator.

ODD Operational design domain.

OEM Original Equipment Manufacturer.

OES Operating Envelope Specification.

PQC Post-quantum cryptography.

QoS Quality of service.

R&D Research and Development.

RFI Request for information.

RFID Radio Frequency Identification.

ROS Robot Operating System.

S&T Science and Technology.

SAE Society of Automotive Engineers.

SBOM Software bill of materials.

SCR Situation-Complication-Resolution.

SDO Standards Development Organization.

SERI Strategic and Emerging Research Initiatives.

SDSM Sensor data sharing messages.

SI International Systems of Units.

SIP Smart Intersection Project.

SOTIF Safety of the intended functionality.

SNR Signal-to-noise ratio.

SPMD Safety Pilot Model Deployment.

SSDF Secure Software Development Framework.

UCEF Universal CPS Environment for Federation.

UNECE United Nations Economic Commission for Europe.

USG NSSCET U.S. Government National Standards Strategy for Critical and Emerging Technology.

USDOT U.S. Department of Transportation.

V2G Vehicle-to-grid.

V2I Vehicle-to-infrastructure.

V2N Vehicle-to-network.

V2P Vehicle-to-pedestrian.

V2V Vehicle-to-vehicle.

V2X Vehicle-to-everything.

VCC Virginia Connected Corridors.

VDOT Virginia Department of Transportation.

VRU Vulnerable road user.

VTTI Virginia Tech Transportation Institute.

Appendix C. Systems Interaction Participant Feedback

The content of the tables is taken directly from the contributions of the workshop participants. The arrangement of the tables does not imply any order of priority; they are organized simply to enhance readability.

Table 9. Feedback on NIST Systems Interaction Testbed Architecture.

Diagram Area	Recommendations
Standards and Use Cases	• Conduct a mapping of standards across the various areas of the architecture to help resolve issues related to cloud, cybersecurity, sensing, and V2I/V2X standards. • Add sample use cases to elicit discussion of key issues that the systems must support/survive to ensure safety (e.g., excess load at one decision A causes issues at point B and C, etc) and guidance on how to test for multiple use cases.
Complexity, Flow, and Completeness	• Remove some of the replications, or assess whether they add value (i.e., the sublayer background is most important). • Continue to review other frameworks for potential application to AVs, and simplify where possible (e.g., Situation-Complication-Resolution (SCR) Framework). • The complexity and volume of text and boxes make it more difficult to track flows. • The flow of data and "input" paths could be clearer (e.g., left to right or top to bottom). • All data flows appear to bottleneck through an ISO/OSI stack. • Categories should be open to additions (both technology and scope) to ensure that they are reasonable and complete.
Human Interactions	• Including human interactions with vehicle systems may be useful in the future. (Note: NIST considered this in previous drafts of the diagram.)

Vehicle Responses and Interactions	• The architecture does not capture actions that may be taken by the vehicle. • Other road users (e.g., vehicles, VRUs, etc) are not part of the design space, but assumptions about these should be integrated. • It is unclear how perception of and itself will provide an adequate measure in how the system views and responds to the environment.
Controls	• Motion planning outputs and controls should be integrated. • Consider whether classical control algorithms should be implemented into vehicle systems and how they would be integrated into this scheme.
Centralized Governance	• The architecture lacks a fully integrated overall monitoring and reporting framework (i.e., primary governance system). • A forensic capability would be useful (e.g., complete details like an aircraft black box to track all signals, inputs, error messages, etc).
General Improvements/ Concerns	• The framework needs to consider issues of interoperability and frequency bands that may be required. • Cybersecurity should be incorporated at the front end of the framework. • The framework is a good start, but new ideas and overlooked concepts should be considered. • The “action” portion of system response is missing. • The systems shown in the framework need to be taken within the context of other AV physical systems and scenarios (e.g., braking, steering, etc).

Table 10. Challenges for Systems Interaction Testing and Characterization.

Category	Challenges and Barriers
Measurement and Characterization	• Ability to measure all the real-world variables (e.g., slick surfaces, human behaviors, inconsistent infrastructure, roads with potholes, shoulders suddenly disappearing, etc). • Measuring system performance versus measuring a singular result or effect. • Lack of standards and metrics for measuring safety (e.g., crashes per miles/hours). • Lack of established measurement criteria for emerging technologies (e.g., AI).
Testing and Communications Standards	• Lack of standards for scenario testing (e.g., adequacy of companies conducting their own tests with their own data; interactions testing is a layer above components testing). • Lack of standardization for both internal and external communications (more challenging to develop internal module communications standards); Department of Defense (DOD) has defined application programming interfaces (APIs) but messages are not generally standardized across vehicle systems. • Limited or no IP addresses for vehicles today. • Inability to plug into the system if there is no open national standard (vendors using same hardware but different software).
Limits to Simulation Tools	• Tools and models used for co-simulation are not AV-specific and may not accurately capture AV interactions internally or with the environment. • Insufficient data to create good models or simulations. • Different topologies, data structures, operating systems, and components between vehicles and systems; models may not be representative.

Testing of System Interactions	• Common interfaces (i.e., same inputs and outputs) required to enable testing among different manufacturers (e.g., braking). • Need to build in ability to change testing as new vehicles and technologies emerge. • Risking safety by simulating a real-world set of inputs without having tested in the real world; vehicle interactions are inherently volatile and unpredictable. • Contributions to "how safe is safe" are limited to full system performance in testing. • Lack of safe, closed testbeds that are open to all developers. • Insufficient data on interactions to test for solutions. • Difficulty identifying priority scenarios.
System and Data Complexity	• Difficult to process, store, and analyze massive raw data and data flows on-network in real time. • Multiple subsystems beneath major components will complicate ability to simulate, capture, and test responses: – Multiple different sensors producing data at different speeds, resolutions, and uptake rates and feeding into perception modules to produce outputs consumed by AI; control and decision-making.
Intellectual Property/System Access	• Limited or no data access to OEMs and restricted vehicle networks, which are usually proprietary and monetized. • Government regulations may be needed to enable some data access. • Proprietary concerns and lack of guidance may influence the outputs of interaction testing.
AI	• Unexpected behavior of AI if "over-trained" or providing unusual responses.

Table 11. Research and Testing Needs for Systems Interaction.

Category	Research Topic or Approach
Co-Simulation Architecture	• Ability of sensors interpret their environment (i.e., sensor metrics). • Dropped sensor input causing AI to misbehave and/or strange input from sensors that could indicate cyber attacks. • Response time and determining whether corrective actions could be planned and executed in time to prevent an outcome that impacts safety (e.g., accident). • Quantifying system interactions that are occurring but not necessarily catastrophic.
Documentation of Interactions	• Applying current regulations (e.g., FDA and DOT) and the NIST Cybersecurity Framework to AVs. • Interaction of multiple AV systems operating in a single area during emergency scenarios (e.g., all stop and wait for instructions).
Testing Capabilities	• Testing that considers the nuances of the real world (e.g., bugs fly into sensors, imperfect infrastructure, many hundreds of things that can go wrong) by using controlled real-world crash testing or simulations with data from prior tests.
System Capabilities	• Ability to dynamically update to select “rural” versus “city” models (e.g., switch a button to go from rural to city, like a slippery to dry button).

Sensors and Data Analytics	• Develop plug-and-play interoperability for standardized data sharing and communications.
	• Develop X-ray sensors to see through vehicles and enable stopping in an emergency.
	• Develop localization instrumentation when GPS is unavailable or inadequate (e.g., dirt roads, raining, no cell tower, bad road conditions, etc).
	  – NIST to potentially explore a repeatable local measurement via a sensing instrument.
	• Understand how much data is actually used and how much IT load is allowable.
	• Research senior fusion for AVs (i.e., measuring various EM wavelengths at different resolutions and at near real-time to provide a cohesive view).
	  – Leverage work in Europe related to information-sharing across vehicles.
	  – Identify and leverage the workable multi-source data fusion systems and frameworks already in operation (e.g., aircraft, space, etc).
	  – Provide direction to the stakeholder community on sensor fusion methods.

Appendix D. Perception Participant Feedback

The content of the tables is taken directly from the contributions of the workshop participants. The arrangement of the tables does not imply any order of priority; they are organized simply to enhance readability.

Table 12. Feedback on NIST Perception Activities.

Category	Recommendations
System Integration	• Address challenges at the system level by combining inputs from diverse sensors and the prediction of actions of other road users. • Determine how to extract information from multiple sensors (e.g., the optimal algorithm for airplanes has been found). • Improve processing speed to amplify the reaction time for predictions. The underlying technology to process data is an essential concern, especially in rural areas with unreliable Wi-Fi. • Enhance the focus on perception algorithms that use raw data to identify objects. • Leverage communication/information exchange between objects. • Determine how to test whether a system collecting information is working optimally.
Technologies Beyond LiDAR	• Evaluate cameras, including event-based cameras. • Include radar. • Include hyperspectral imaging and a database of the spectral signatures of different objects. • Standardize sensor fusion for specific applications (e.g., LiDAR and camera versus LiDAR and radar) to help users identify the best sensors to fuse for particular applications.

Additional Information on Sensors	• Examine the compatibility (i.e., non-interference) of competing LiDAR sensors. • Understand a methodology or technical information that assesses whether LiDAR fulfills the requirements of AV perception. • Answer questions about latency. • Characterize noise factors on sensors.
Miscellaneous	• Develop terminology for levels of classification (from a thing to a vehicle to a Red 1992 Ford Mustang GT). • Define acceptable levels of perception accuracy. • Focus on security and safety. • Use data for collision reconstruction. • Develop testing procedures for AVs to support sensible policies.

Table 13. Challenges and Barriers for Perception.

Category	Challenges and Barriers for Perception
Edge cases that pose a challenge to existing AV perception sensors or a fusion of these sensors	
Technical Challenges	• Challenging SNR situations. Since radar and LiDAR have variable power, near- and far-field measurements are needed. These circuits usually have time responses, so situations in which reflectance changes rapidly or targets are revealed quickly are difficult. Characterizing the nature — not just the level — of noise is important. • Interference from other sensors, environmental factors, or attackers requires a failure mode and error handling. Secondary sensors would also help improve failure modes. • Developing perception logic that can work with imperfect information, as perfect sensors cannot be created. • Mixing measuring equipment (e.g., LiDAR) with detection and identification logic. • Maximum number of objects/targets that a system can detect at once (varies with sensors).
Data Challenges	• Data corruption and data quality, accuracy, and validity (e.g., if a perception system detects a car, is the car really at the detected distance?). • What can or cannot be reliably perceived local to the AV versus a more collaborative perception. • Data annotation across multiple modalities.
Sensor Fusion	• Sensor fusion that creates blind spots and blurring (e.g., LiDAR is good for detecting objects in mid to far ranges, and cameras are good for classifying objects in close to mid ranges, but a fusion of the two will have a dead band for a perception system fail). • Identifying likely cases of poor sensor fusion (e.g., sensors contradicting themselves) and strategies to address them. • Imagers and combinations that are good in static situations but not dynamically.

Object Detection	• Crowded streets with different types of vulnerable road users (VRUs) (e.g., pedestrians, bicyclists, skateboarders, etc). • Items in the roadway that are not normally present (e.g., animals, blown tire fragments, parts falling off cars, fallen power lines, police tapes, fire hoses on the ground). • Negative obstacles (e.g., potholes). • Unrecognizable patterns (e.g., a white reflective ball, reflective and retro-reflective items, color, lights, LEDs).
Occlusion	• The occlusion spot, where vision is obscured (e.g., the need for an "x-ray" sensor that can detect the car braking two cars ahead of the AV). • Range of detection of objects crossing paths (e.g., detecting around corners). • Classification of occluded objects.
Weather and Time of Day	• Extreme weather that affects sensor response (e.g., extreme rain that reduces visibility or snow that occludes cameras). • Technologies that cannot be used on snowy roads (e.g., ground-penetrating radar could help identify the road surface but needs to work at higher speeds). • Poor vision at night. • Sun low on the horizon. • Heavy sunlight (can affect LiDAR performance).
Barriers for adoption of perception sensors for automated driving	
Technical Barriers	• Challenges with integration into the vehicle (e.g., data overload, reliability, maintenance, and calibration). • Limited ability to measure the performance of new technologies. • Poor sensor output (e.g., LiDAR can see a sign but cannot read the text on the sign). • Interoperability challenges.

Market Barriers	• The high cost of accurate perception sensors (e.g., LiDAR and cameras). • The number of sensors on the market and limited knowledge of their performance and limitations in various environments. • Proprietary technology and blackbox solutions. • Liability concerns that prevent mass adoption, especially for small businesses.
Standards to Enable Private-Sector Development	• Need for a standard that allows different vendors to produce products with varying capabilities and that provides a practical baseline perception system requirement. • Need for a standardized baseline to compare nominally similar types of sensors. • Need for a standard procedure to systematically calculate the number of sensors based on their efficiency and the extent and proportion of fusion required to drive in a set of conditions. • Need to identify a minimum number of wavelengths and which wavelengths are needed for automotive obstacle classification to enable the development of low-cost solutions (e.g., agriculture drones with 4 to 12 wavelengths, depending on what they need to detect). • Need for a clear definition of “proper sensor operation” and transparent testing. – NIST can establish a testbed or procedure for sensor testing with known uncertainty and use results to certify systems and their components. • Need for a full testing environment that adequately matches real-world environments since small businesses do not have the capital to install a closed track (e.g., sensors on a moving “vehicle,” hardware and software that can process the input, and hardware and software to send the output of the resulting reactions).
Consolidation in terms of sensor technologies	

Possible Consolidation	• Recent advances in event-based cameras for automated drone flight, which may be transferable but require capable systems and are often classified. • A move toward solid-state LiDAR, though mechanical detection solutions (e.g., motor-driver LiDAR) are more prone to failure.
No Consolidation	• Proliferation rather than consolidation (e.g., more wavelengths, more modulation techniques, new sensor types). • Need for multiple sensors with complementary limitations and strengths. • Need for interoperability rather than consolidation.

Table 14. Research and Testing Needs for Perception.

Category	Research Topic or Approach for Perception
Parameters/aspects of AV perception sensors that need standardization and standards currently in use	
Sensor Performance Requirements	• Minimum performance requirements (e.g., latency, false positive rate, false negative rate, maximum objects detected, etc). • Minimum technical specifications (e.g., refresh rate, image quality, frame rate, range, lag time, etc). • Standards for AV's ability to see items or the infrastructure as designed for humans: – Distance. – Cone of vision, including horizontal and vertical angles. – Color detection (at least all of the colors in the Manual on Uniform Traffic Control Devices for Streets and Highways (MUCTD)). – Lighting (e.g., LEDs, and automotive, street, and traffic control devices). – Dark, dusk, and day variations. – Weather and other environmental particulates. • Focus on results (e.g., detecting a stop sign 20 meters away, detecting traffic light color 50 meters away) rather than LiDAR (or any specific sensor type). • IMU sensors give a 10- to 20-second window (when accurate) to transition to ADAS operation. • Interoperability, communication, and interference.
Other Sensor-Related Topics	• Standards for any sensor that can affect other vehicles (e.g., how to mitigate LiDAR interference) • Standards for spectrum allocation (i.e., frequency of allowed radar changes) for each country, though standards for particular parameters. (e.g., frequency) may not be possible. • Bandwidth and handing cost-related processing selection.

Other Systems	• Standards for AI systems that support AV perception and address how well the system should work to provide "guarantees" to users or regulators. • Infrastructure (e.g., changes in signage, LiDAR on roadside, reflective paint, etc). • Perception logic (e.g., output standardization and explainability, which is also helpful for collision reconstruction). • V2X standardization to help facilitate and prioritize implementation.
Infrastructural changes and resources needed to augment AV perception sensors	
V2X, V2V, V2I	• Internet of Things (IoT) advance to enable robust communication and information exchange and provide another sensor modality, especially for visually challenging environments: – Traffic lights that can broadcast color, direction, time to change, etc – Temporary traffic lights. – Ability to check whether signage is blocked by trees. – Changes in the roadway (e.g., during road construction). – Ability to identify a valid stop sign. – Ability to navigate in extreme environments and through variations in lighting. ∗ A standardized way to have infrastructure work in tandem with the vehicle (e.g., putting up sensors on a road undergoing construction); OEMs and other developers do not trust infrastructure (especially V2X) to work consistently. ∗ V2V and V2I communication to ensure that data cannot be misinterpreted (e.g., spoofing attacks) and avoid a singular vehicle sensor/logic point of failure. ∗ Implementation of 6G, or "real-time", data flow.

Roads and Signs	• Roads designed and built specifically for AVs and note problem areas (e.g., traffic circles, intersections, construction zones, the unexpected).
	  – Modifications to the MUCTD so that road signs are not modified or spoofed.
	  – Signs specific to AVs (e.g., using infrared QR codes).
	  – Radio Frequency Identification (RFID)-type tags that can be applied to signs, roads, streetlights, or intersections with information on their precise locations.
	• QA database combined with AI that involves regular checks of each road and path as inputs and can be fed into independent AI within AVs.
	• Infrastructure maintenance (e.g., faded lines, broken reflectors, missing signs, and other inaccurate or missing input that can lead to AVs behaving incorrectly).

Other Uses of Data to Improve Sensor Functionality	• AI feedback delivered through infrastructure services that supports or improves the decision-making of AV perception sensors (including the relevant software logic). • Ways to prioritize data in a given scenario and/or determine which sensors to trust at any given moment (e.g., sensors could output confidence measures to help with determination). • Reference targets that allow a sensor to self-diagnose. • Public datasets that include images and scenarios of challenging environments to help train and compare the performance of different perception algorithms.
Miscellaneous	• Emergency vehicle light standardization (e.g., color, frequency, size, light location, design, sound) for better detection. • Synchronized AC LED frequencies since taking images at different rates may not create a full image.
Gaps in technical specifications	

Assumptions	• Standards should focus on the desired outcome (e.g., detect objects with x % accuracy) rather than the sensor, and the pros and cons of each sensor capability should be well-documented. • Uncertainty is built into any AI-based classification system. • Defining "failure" (e.g., it is not a failure unless the system is based entirely on image classification) and using more useful terms (e.g., false positives, misclassification, etc).
Sensor Fusion	• Knowing the bounds of individual sensors and how to combine the capabilities of multiple sensors to achieve ideal performance and meet requirements. • Ability to dynamically change the fusion depending on the environment. • Limited understanding of how uncertainty in one sensor is affected if you fuse multiple sensors (i.e., if you have uncertainty in multiple sensors, the collective uncertainty of a system is not guaranteed to be bounded).
Sensor Sight Limitations	• Standard specifications for positioning and minimum sensor performance (e.g., whether AVs are able to see the roadway horizontally and vertically for intersections, exits, entrances, and merge/weave dynamics). • Static sensors that do not handle enough of the challenging situations. • Sensors limited to line of sight.

Understanding AI	• Understanding how deviation translates into output and how it is connected to the level of discrepancy. • Use of conditional learning or a robust neural architecture to imitate an expert human driver and superimpose automatically generated policies for uncertainty (e.g., run time) with confidence levels that can be changed based on conditional changes. • Trained network that combines sensor fusion with AI. • Continually testing and updating any AI-based system. • Specified uncertainties in the data itself for AI-based detection.
Miscellaneous	• Terminology to determine whether sensors are more or less deterministic (e.g., Doppler LiDAR and hyperspectral can deterministically measure velocity). • A standard method that compares the performance of sensors of the same sensor type. • System agility. • Certification tests.

Appendix E. Cybersecurity Participant Feedback

The content of the tables is taken directly from the contributions of the workshop participants. The arrangement of the tables does not imply any order of priority; they are organized simply to enhance readability.

Table 15. Feedback on NIST Cybersecurity Efforts and Additional Areas of Research.

Topic Area	Comments and Recommendations
Additional Cybersecurity Considerations	• AML and generative adversarial networks (GANs), though GANs may not be the most feasible considering cost-effectiveness, productivity, and hacker use of these tools. • Consider the overall flow of data into and out of AVs (e.g., for V2G plug and charging process) and incorporated into hardware and software security and standards. • Increase focus on common AV components beyond AI (e.g., vehicles being hacked or unlocked using various approaches, such as a laser into a sensor/camera or a specific frequency into a microphone). • Physical attack vectors (e.g., wires, sensors, ports, etc) that can be accessed inside or outside of the vehicle and are more likely to occur with AVs than in traditional IT. • Communication with handheld devices and 5G security. • Teleoperation (e.g., a trucking company talking to fleet) and platooning (e.g., driverless trucks following a lead truck). • Apply the concepts learned from static systems to fast-moving, real-time in-vehicle network (IVN) anomaly detection for AVs. • Forensics support for post-hack analysis. • Optimized monitoring, tracking, and reporting (e.g., designing digital twins to examine how attacks happen and are responded to).
Long-Term Software Support	• Long-term support for cybersecurity should extend throughout the vehicle's expected life cycle (i.e., 10–15 years), such as code signing and requirements that software be kept current and available over similar time frames.

Existing Cybersecurity Standards	• Leverage existing cybersecurity standards (e.g., increase NIST's focus on metrology to address issues). • NIST's SSDF, ISO 26262 (safety in road vehicles systems), SAE/ISO 21434 (vehicle cybersecurity, joint standard), ISO 21448:2022 (road vehicles), and UNECE Regulation R155 (cybersecurity). • Create mappings across relevant ISO standards and NIST in the AV cybersecurity space.
Additional Suggestions	• Host workshops focused solely on AV cybersecurity issues. • Apply AI security concerns to specific AV use cases . • Integrate cybersecurity into sensor testing. • Ensure that feasible cybersecurity measures are in place when security is breached, which is especially challenging when systems must be fail-operational (e.g., ability to identify compromised systems and determine whether they can operate safely when sensors are compromised). • Address fundamental root causes that affect security (i.e., constructing products to be fundamentally secure) rather than focusing on external attackers and defenders. • Emphasize privacy concerns to encourage adoption (e.g., LiDAR takes in a very high resolution of information, such as capturing license plates), and tag and encrypt shared data. • Ensure that cybersecurity is part of the entire design and development process.

Table 16. Challenges for Implementing AI and Addressing Cybersecurity Risks.

Topic Area	**Challenges for AV Cybersecurity**
AI Decision-Making	• AI/ML may not yet be mature or robust enough for use since they can be fooled (e.g., through adversarial object recognition). • Misuse of AI can cause vulnerabilities and is a big issue for all applications.

AI Safety	• Potential opportunities in "Cyber Safety" — combining research on cybersecurity methodologies and functional/system safety methods with safety of the intended functionality (SOTIF). • AI-based testing could improve understanding of AI-based security safeguards and generate better test cases.
Cyber Attacks	• AI's capability to redo and improve hacking algorithms to invade a system. • The complexity of AI systems and the inability to exhaustively verify them may make the misbehavior of an AI system indistinguishable from a malicious attack. • Difficult to identify malicious actors prior to hacking since insecurities and vulnerabilities are determined based on the general hardware or software systems. • Building cyber resilience.
Personal Privacy	• Personal privacy considerations since vast amounts of information will be collected by cameras, sensors, and GPS and potentially transferred off-device.

Table 17. Research and Testing Considerations for Overall Vehicle Cybersecurity.

Topic Area	**R&D for AV Cybersecurity**
Privacy Concerns	• Prioritize cellular and physical access ports over common IT objects (e.g., Ford's self-driving system detects one's face while driving), and determine how information is stored and used. • Ensure that data collected from outside of the vehicle is aggregated and anonymized to protect individual privacy (e.g., NIST recommendation that every vehicle send a BSM).

Safety Considerations	• Identify failsafe mechanisms for cyber resiliency (e.g., ADAS would need to keep operating in incidents, such as signal jamming). • Identify acceptable standards for reporting security incidents. • Potential for blackbox monitoring system to allow for full post-event analysis with centralized reporting for isolation or event correlation across all vehicles on the road.
V2I Considerations	• Awareness that vehicles will also have other connections (e.g., cellular, Wi-Fi, etc). • Importance of cybersecurity measures regarding how systems interact with infrastructure (not just the vehicle). • Transferring data can be a point of attack during AV charging. • Use of redundant sensors to help address these challenges. • Assurance mechanisms for GPS time to prevent miscalculations, vehicle mispositioning, or issues with communication lines (e.g., Assured Positioning, Navigation, and Timing (A-PNT)). – NIST has work going on in this area. • Potentially use blockchain to secure communications (may have a tremendous processing power requirement to ensure verification).
Additional Comments	• Application of lessons learned about industrial control systems (ICSs) (e.g., ISA/IEC 62443 relates to the cybersecurity of ICS; Idaho National Laboratory working on ICS cybersecurity and safety-critical systems, such as nuclear power plants). • NIST-established performance metrics to assess the cybersecurity of AV modules. • NIST's role in ensuring that security standards are met throughout the vehicle manufacturer's supply chain through a bill of materials (BOM), software bill of materials (SBOM) or similar documentation (e.g., UNECE Regulation No. 155 on cybersecurity).

Appendix F. Communications Participant Feedback

The content of the tables is taken directly from the contributions of the workshop participants. The arrangement of the tables does not imply any order of priority; they are organized simply to enhance readability.

Table 18. Proposed Additions/Improvements to NIST Communications Activities.

Category	Comments and Recommendations
Standardization Efforts	• Standardize the frequency of communication for V2X, V2N, and V2P, and set valid communication protocols for authentication and trust. • Create consistent international standards that are aligned with relevant existing standards (e.g., ETSI A-ITS, AES, ISO). • Set standards to ensure that the bandwidth of sensors is not flooded, which could cause degradation or misinformation. • Consider a variety positions and recommendations (e.g., USDOT, 5G Automotive Association, SAE 3161-1, and SAE 3161-0). • Identify best practices relative to vehicle performance and features, and incorporate owner-operator perspectives (e.g., likelihood of communication failures and best responses to system failures).
GPS and Navigation	• Free V2X from the use of GPS (i.e., find or study alternatives to GPS), which is not available in some situations, can be unreliable, and can be easily spoofed with cheap hardware). – Landmark navigation, such as those used by the military (e.g., cooperative localization, locations of trees in forested areas, etc). – Evaluation of various other alternatives – Harmful interference from other objects (not necessarily vehicles).

Technical Capabilities	• Identify best practices for data compression, speed, security, and accuracy in communications. • Test and evaluate one or more C-V2X chipsets from different companies. • Conduct benchmarking on smart grids with NIST-developed measurements
Collaborative Organizations	• Collaborate with other organizations, such as: • Large telecommunication companies (e.g., Apple, Qualcomm, etc,) with AV interests. • Government agencies (e.g., FHWA Office of Safety and Operations R&D, NHTSA, US DOT OST, FCC). • 5G Automotive Association. • SDOs (e.g., SAE Vehicle Communications Steering Committee). • Intelligent Transportation Society of America (ITSA). • Vehicle OEMs, suppliers, and trade groups. • Crash Avoidance Metrics Partners (CAMP) LLC led by GM and Ford.

Table 19. Challenges for AV Communications.

Category	**Challenge**
Measurements	• Generic performance measures to compare and test products as part of a system. • Interoperability evaluation.

Standards	• Limited alignment of EU and US standardization activities; mapping of ISO and IEEE standards with NIST activities.
	• Metrics that are measured differently in standards (e.g., reliability or availability), creating an assessment gap, or not measured at all.
	  – Lack of stratification of standards and performance metrics related to connectivity.
	  – Overly conservative V2X concepts for latency (e.g., less than a tenth of second latency safety-critical applications that may be supported are a small subset of the V2I space).
	• Difficulty in trying to bridge gaps between standards and different countries (gaps are not well-mapped between standards globally).
	• Performance variations when certified components are integrated within a system.

Integrating Communications with Infrastructure	• Distinguishing between V2I and V2V realms, contexts, and domains (e.g., some countries use the cellular system for payment or to fund AV developments). • Challenges of developing cooperative localization and perception (e.g., lack of functionality on roadway networks). • Use of cellular networks for non-time/safety-critical communications (can cause traffic problems even now). – Insufficient authoritative test data from an independent testing authority to support claims for additional dedicated spectrum. • Infrastructure availability. • Spectrum limitations, particularly capacity and connectivity/distance (i.e., how far communication can reach). • Dependence on cooperation with an unreliable and inconsistently maintained infrastructure (e.g., 25,000 local jurisdictions in the U.S., poorly maintained roads, markings, etc).

Reliability	• Managing signal interference, overlap, latency, and hacking issues (e.g., illegal transceiver getting/sending information or blocking signals). • Data blind spots, which could be intermittent (i.e., dead spots with expansions in time and space during/after events that impact reliability).
Government Mandates	• Industry will not mass produce without a guaranteed market. • Regulations tend to be technology-agnostic, making it harder for investors to decide where to invest (e.g., DSRC vs C-V2X).

Table 20. Proposed Approaches for Research/Testing of AV Communications.

Category	**Research Topic or Approach**
Testing Capabilities	• Improvements to test facilities for V2V that are mockups or city surrogates (based on plywood that is not representative of real buildings). – Test setups for signal research (e.g., cargo containers are now used in Japan for AV testing). – Testing where signal propagation is representative of practical situations. • Tests of QoS, security, and latency (minimized interference). • Testing with multiple radios sharing the channel and simultaneously communicating in a challenging environment (e.g., urban canyon, multi-path, restricted GPS, etc). • Ability of communications technology to support the intended ODD of the ADS. • Tests for availability (e.g., mean time to recover, incident response time after cyber attacks, traffic jams, collisions, outages, etc). – Current baseline and how to make it shorter. – Testing and backup plan if AV is compromised. – Driver or vehicle time to regain control after a collision. – Denial of service (e.g., unavailability, where sensors are jammed, etc).

Scenarios for Testing and Research	• Mean time to remediate (MTTR) and related metrics. • Places where communication can fail (e.g., intersection scenarios, occluded spots, harsh weather conditions). • Infrastructure conditions (e.g., tunnels, bridges, urban canyons, etc). • Overall system reliability (i.e., the level that each safety feature requires to be reliable and effective). • Electronics optimization and testing in harsh conditions (e.g., traffic jam, bad weather conditions, etc). • AV and infrastructure systems with built-in redundancies, the ability to navigate independent of V2I, and the ability to use both its own perception and the infrastructure.
Simulations	• Metrics simulators. • Simulation-based evaluation since it is impossible to physically test the number of actors and scenarios stretching the system. • Simulations that are validated against real-life observations.

Appendix G. Artificial Intelligence Participant Feedback

The content of the tables is taken directly from the contributions of the workshop participants. The arrangement of the tables does not imply any order of priority; they are organized simply to enhance readability.

Table 21. Feedback on NIST Artificial Intelligence Current Work and Programs.

Category	Comments and Recommendations
Industry Collaboration	• NIST should engage and convene all types of stakeholders related to AVs, including those in and out of conventional automotive industry, academia, government agencies, and other industries. • Engage the engineering side of AV companies to gain a better sense of what work is being done on these issues. • Consider other fields to learn from (e.g., data from medical devices).
Communication and Information Sharing	• NIST should create a standardized language to facilitate cross-industry communication. • NIST should encourage more public resources and datasets, which are critical to the evaluation of uncertainty metrics since organizations may be reluctant to share. • There should be a more robust labeling system for different objects.
Diversifying Approaches and Focus Areas	• NIST should consider areas other than deep learning and help the community understand potential impacts. • Common-sense reasoning could make AI systems more robust. • NIST could take a more monitoring-based approach rather than being more prescriptive, such as taking an existing AI system and evaluating its metrics independent of the specifics of the model.

Table 22. Challenges for Artificial Intelligence Testing and Characterization.

Category	Challenges and Barriers
Edge/Corner Cases	• Ability to robustly identify people in edge scenarios (e.g., children at play, workers performing various tasks, emergency workers, etc). • Effective methodology to identify real-world corner or edge cases to develop confidence that the system can behave appropriately in these cases.
Computational Overhead and Real-Time Processing	• Consideration for the limited computational resources in AVs. • Alignment of multiple interacting systems, each with their own latency. • Real-time object detection and overlapping computations.
Changing Environment	• Weather conditions (e.g., electromagnetic interference (EMF) issues that affect sensors, darkness). • Roads conditions (e.g., construction, accidents). • Impact of many AVs on the road (e.g., LiDAR interference, etc). • Overfitting a system to a specific locale. • Partial occlusion (i.e., systems trained to detect people and objects based on full images).

Sensor Fusion and Communication	• Sharing information about the same scene from different viewpoints using advanced V2V communication and compression techniques (e.g., Octree compression) to wirelessly send rich data. • Unclear how a vehicle will make a decision based on collective data. • Multi-modality (e.g., camera, LiDAR, thermal, etc) to enhance robustness, though modalities other than vision have fewer comprehensive datasets and may be far more expensive (e.g., thermal). • Developing new sensor types versus increasing the robustness of existing ones. • Addressing overlapping sensors with functions that differ from their original designs and require adaptation.
Data Collection and Availability	• Comprehensive and diverse datasets for generalization, including public datasets. • Reclassification for data collection, which currently focuses on detection algorithms and is not always integrated with control systems. • Exploration of alternative datasets since some data modalities (other than vision) may face limitations. • Use of multi-modality (e.g., combining camera and LiDAR data) to enhance AI robustness.

AI Safety	• AI/ML to improve robustness given the data input and challenges around system safety and safe behavioral responses to different input conditions (e.g., vehicles stopping without clear cause and resulting in traffic issues, recognizing an actual stop sign versus a paper sign). • Certification processes could require an explanation of how AI systems work and why they are safer. • Ensuring safe fallback modes, implementing a set of constraints for the AI system's feedback into the vehicle (i.e., a predetermined set of "okay" responses), and limiting AI and ML models so that they do not take up the entire system and lag safety-critical responses (e.g., driver assistance versus fully autonomous, leveraging AI similarly to how ADAS sits on top of existing mechanical systems).
AI Decision-Making	• Verifying the quality and fidelity of data used by AI systems and continually updating training and communications data as part of the cost of AI. • Quantifying decision paths for testing adjustments in AI models (i.e., range of aberrant behavior). • Statistical (rather than deterministic) model for tested decision boundaries and deterministic fail-safes.

Table 23. Research and Testing Needs for Artificial Intelligence.

Category	Research Topic or Approach
Utilizing Real-World Data	• Utilize untapped data from Transportation Operation Centers, which receive significant data streams (e.g., camera feeds), for training sets and system models, especially object recognition. • Use data reduction practices that involve human labeling and annotation, and harness human-labeled datasets from real-world driving for ground-truth comparisons. • Use controlled setting or test track data collected with intentionally depleted environments (e.g., rain, snow, fog, partial obstruction, various lighting conditions).
Outreach and Collaboration	• Bring various AI-related standards groups together with automotive/transportation-focused standards groups (e.g., ISO/JTC 1/SC 42, ISO/TC 204, ISO/TC 22, and SAE committees) to promote information exchange and collaboration in advancing standards. • Engage communities to design specific road scenarios for benchmarking test cases. • Aggregate and average data from different neural networks. • Train a multitude of networks. and conduct statistical processing.
Changing Environment	• Weather conditions (e.g., electromagnetic interference issues that affect sensors, darkness). • Roads conditions (e.g., construction, accidents). • Impact of many AVs on the road (e.g., LiDAR interference, etc). • Overfitting a system to a specific locale. • Partial occlusion (i.e., systems trained to detect people and objects based on full images).

Ensemble Methods	• Aggregate and average data from different neural networks. • Train a multitude of networks. and conduct statistical processing.
Standardization Efforts	• Develop a basic competency test for these systems. • Utilize a spectrum of testing approaches. • Create an open-source code to develop testing methodologies for evaluating model performance in specific scenarios and conditions, and standardize methodologies for evaluating them. • Develop a standard set of metrics to mathematically articulate what is safe or unsafe and to evaluate these systems and vehicles. • Create a taxonomy of classification (e.g., defense circles define detection, discrimination, distinction, etc) with the understanding that not all use cases have the same level of need when it comes to object classification. • Design specific road scenarios for benchmarking test cases.

Appendix H. Resources

- (White House May 2023) U.S. Government National Standards Strategy for Critical and Emerging Technologies. https://www.whitehouse.gov/wp-content/uploads/2023/05/US-Gov-National-Standards-Strategy-2023.pdf
- (White House May 2023) FACT SHEET: Biden-Harris Administration Announces National Standards Strategy for Critical and Emerging Technology. https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-national-standards-strategy-for-critical-and-emerging-technology/
- (NIST 2023) Standards and Performance Metrics for On-Road Automated Vehicles Workshop.
  - Event Information: https://www.nist.gov/news-events/events/standards-and-performance-metrics-road-automated-vehicles-workshop
  - Presentations: https://www.nist.gov/el/intelligent-systems-division-73500/standards-and-performance-metrics-road-automated-vehicles
- (NHSTA 2023) Standing General Order on Crash Reporting. NHSTA April 2023.
  - General site information: https://www.nhtsa.gov/laws-regulations/standing-general-order-crash-reporting#:~:text=NHTSA%20has%20issued%20a%20Standing,2%20advanced%20driver%20assistance%20systems
  - PDF of Standing Order: https://www.nhtsa.gov/sites/nhtsa.gov/files/2023-04/Second-Amended-SGO-2021-01_2023-04-05_2.pdf
- (ISO 26262) ASIL D, automotive risk classification that is part of a larger ISO standard – ISO 26262 and looks at the functional safety requirements for all of the different electrical and electronics systems in a vehicle. https://functionalsafetyengineer.com/introduction-to-asil/