Summary of NIST's Current Progress in Standards and Performance Metrics for On-Road Automated Vehicles

National Institute of Standards and Technology (NIST)
September 5th to 8th, 2023

Introduction

Automated driving systems (ADS) and automated vehicles (AVs) have the possibility to affect key aspects of society including transportation, goods delivery, manufacturing, public safety, and security. Measurement science and standards are needed to support the safe and predictable operation of AVs, which may pose a risk if these complex systems do not perform as expected. US industry and other government agencies have been looking to the National Institute of Standards and Technology (NIST) to develop test methods, metrics, and standards to characterize the performance of these complex, cross-disciplinary, and cross-sectional systems to support AV development and mitigate risk to vehicle and component manufacturers as well as public consumers. In 2022, NIST held the Standards and Performance Metrics for On-Road Autonomous Vehicles Workshop to solicit stakeholder feedback with respect to challenges and opportunities in developing standards and performance metrics for AVs.

The workshop identified several key areas in which NIST could have an impact. Over the past year, NIST has started to perform research and explore performance metrics and standards in a number of those areas. The purpose of this workshop is to bring together the AV community to update them on NIST's recent work, provide a forum for stakeholder feedback, and set a path forward to ensure that NIST's efforts contribute the greatest value to the community. The following describes NIST's progress in the AV fields of systems interaction, perception, cybersecurity, communications, and artificial intelligence (AI).

Systems Interaction

Problem Statement

Although there are existing limited system-level tests that evaluate individual components including sensor suites and communication layers, as well as overall vehicle testing on dedicated tracks, stakeholders have recognized the significance of assessing the interactions between these systems, which significantly impact the overall vehicle performance.

Such a testbed would be useful to stakeholders to transition individual system-level testing to overall vehicle performance while reducing design and validation iterations. However, a community consensus to perform this testing does not currently exist. NIST's mission is uniquely suited to provide unbiased system-level testing owing to its measurement expertise across a wide array of research domains. Therefore, NIST's thrust in Systems Interaction aims to provide stakeholders with an evaluation framework for system interaction testing in automated driving supplemented with corresponding testbeds.

What NIST has Done

Automated Driving Systems Interaction Evaluation (ADSIE) Framework

To date, NIST is developing an Automated Driving Systems Interaction Evaluation (ADSIE) framework. The ADSIE framework currently stands upon 6 pillars as follows (with examples):

- Systems: Camera, lidar, V2V
- Environmental Scenario: Sunny day in metropolitan environment with three vehicles
- Behavior Assessment: Lane following, emergency braking, adaptive cruise control
- Evaluation Metrics: Distance from obstacles, communication bandwidth, velocity profile
- Perturbations: Communication overload, cyber events, adversarial AI
- Uncertainties: Object uncertainties, obstacle uncertainties, system failure modes

The ADSIE framework enables stakeholders to create, evaluate, and implement testing scenarios aimed at capturing the system interaction performance of automated driving features. Such a framework aims to accelerate the manufacturing and adoption of automated driving technologies by providing holistic yet detailed understandings of vehicle performance in laboratory and real-world environments.

Systems Interaction Testbed

To provide example scenarios of the ADSIE framework, NIST has developed the simulation infrastructure for a Systems Interaction testbed. This simulation testbed is intended to be used by stakeholders for evaluation. The simulation infrastructure consists of the following[1]:

- Driving scenarios and environments with CARLA
- Automated driving functions operated by Autoware
- Flexible software publish/subscribe messaging using ROS
- V2X communication infrastructure managed by the NS-3 network simulator

[1]Certain commercial equipment, instruments, or materials are identified in this document in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

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

Next Steps

NIST aims to prototype a physical systems interaction testbed (a development mule) using the lessons learned by the ongoing effort in addition to solicited stakeholder feedback. Through this physical testbed, stakeholders will be able to leverage NIST resources for systems interaction testing in addition to understanding the ADSIE framework. NIST also aims to engage stakeholders and foster communities from the multiple stakeholders within the various automated driving stacks.

Tentative Breakout Discussion Questions

- What do you recommend we should measure from co-simulation architecture?
- What scenarios do you think would benefit from this automated driving system interaction evaluation framework?
- Do you feel that the presented diagram is useful towards understanding NIST's approach?
- Do you think that the proposed systems (cybersecurity, AI, perception, communication) are enough to capture AV system interaction?
- Do you think there is a need for standardization for documentation/metrics/test methods of capturing how the AV systems interact?

Perception

Problem Statement

Safety of autonomous vehicle operations are heavily dependent on sensors, systems and technologies which form the "eyes" for these vehicles. For this reason, it is important that these systems provide high fidelity data with low uncertainties and latencies, and that are robust and tamper-proof. The performance of these systems is also dependent on external factors such infrastructure, weather, lighting conditions, etc. Evaluating such systems is still fraught with ambiguity.

What NIST has Done

The AV Perception project has developed a testbed and is developing methods for evaluating the performance of perception systems for automated vehicle applications. The initial focus of this work has been AV lidars in static indoor environments.

Data Acquisition Pipeline

A common data acquisition pipeline was developed by using ROS2 as the middleware on a Linux operating system. One of the initial challenges was to find the appropriate software drivers (ROS2) for acquiring the data from lidars. It was discovered that there are no officially supported ROS2 drivers for the lidars used for this project and the 3rd party drivers exhibited performance issues such as dropped packets and data fidelity.

Evaluation Procedures

Lidar evaluation procedures were performed using:

- SI traceable artifacts such as white/black target boards
- Calibrated spheres that were measured using CMMs
- Laser tracker that offers sub-millimeter uncertainties at sphere-sphere lengths <10 m

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

Next Steps

The initial focus of this project has been developing a testbed and evaluating lidars in static, indoor environments. The next steps in this work are to perform these tests in outdoor and dynamic environments. Apart from these, various Simultaneous Localization and Mapping (SLAM) algorithms will be evaluated to understand the contribution of algorithms in localizing the vehicle on which the lidar is mounted.

Tentative Breakout Discussion Questions

- What parameters/aspects of AV perception sensors need standardization in the near future (as a priority) to accelerate their adoption?

- What are the edge cases that pose a challenge to existing AV perception sensors or a fusion of these sensors?
- What are the barriers for adoption of perception sensors for automated driving?
- Does present computing hardware present a barrier for effective use of sensors and sensor fusion?
- What kind of infrastructural changes and resources are necessary for augmenting AV perception sensors in challenging environments?
- Are there any gaps in the technical specifications of perception sensors and their performance?
- What standards are being used to evaluate perception sensors for performance, acceptance testing?

Cybersecurity

Problem Statement

AVs take the software-based vehicle to its logical extension and, therefore, increases cybersecurity risks. As machine learning (ML) and AI systems have become more widespread, managing the unique risks of ML systems to achieve trustworthy operation is a challenge that organizations now need to address. In addition to managing the infrastructure upon which ML systems operate using traditional cybersecurity principles, a range of new possible vulnerabilities need to be mitigated. Establishing the trustworthiness of an ML model is especially hard because the inner workings are essentially opaque to an outside observer. Ideally the models we rely on would be transparent, free from bias, explainable, and secure. Research has shown that ML models are vulnerable to a variety of adversarial attacks that cause them to misbehave in ways that provide benefit to an adversary. This vulnerability of ML models has sparked a growing challenge for securing ML systems due to the competition between defenses attempting to mitigate attacks and ever novel attacks that defeat the defenses. In addition, once a vehicle has been manufactured and purchased, there is on-going maintenance which includes software updates. At one time, all such updates were downloaded through tools supplied by the Original Equipment Manufacturer (OEMs) and applied by mechanics in garages. Now, OEMs are looking to take advantage of over-the-air updates into vehicles. As with IT equipment, such updates represent an attractive target for adversaries. Concerns about updates as a source of attacks have led to substantial standards work over the last few years.[2]

What NIST has Done

Improve Communications with Industry

To help the automotive industry keep up with NIST's cybersecurity activities, NIST has developed the Automotive Cybersecurity Community of Interest (AutoSec COI). This community is designed to allow access to NIST cybersecurity work in a lightweight fashion. Announcements covering a range of NIST activities are sent to the AutoSec COI, allowing members an easy and convenient way to receive information on NIST cybersecurity activities. The AutoSec COI also offers monthly webinars that showcase on-going cybersecurity work at NIST.

Cybersecurity of AI

Dioptra is a software platform that aims to foster a principled approach to the characterization and evaluation of ML systems under a diverse set of conditions. To that end, it has a modular design enabling researchers to easily swap in alternative datasets, models, evaluation methods, attacks, and defenses. Dioptra is a freely available open source software platform that is deployed within a user's own infrastructure to allow users to analyze systems within their own environment without the need to share any data or resources. While the immediate focus has been on the security and resilience of ML models, measurement of other trustworthy characteristics can be easily incorporated. The end result is that Dioptra provides a strong foundation to advance the metrology needed to ultimately help evaluate multiple trustworthy characteristics of AI/ML-enabled systems.

Code Project

The push to automated vehicles and automated driving systems have increased the importance of software and firmware integrity in the automotive industry. With each passenger vehicle having

[2]ISO 24089:2023 *Road vehicles – software update engineering*; UN regulation No. 156 – *Software update and software update management system*

an increasing cyber footprint to support these automated functions, NIST is considering developing guidance on security techniques and processes to help assure the integrity and authenticity of this software during development, distribution, and update processes. This workshop will focus primarily on the use of cryptographic techniques, including digital signatures in a secure software development lifecycle, to reduce cybersecurity risks in both the supply chain and the operations phase of vehicles' lifecycle. Subject matter experts in the automotive industry will share the existing challenges, industry standards, and proposed approaches for addressing software integrity. The findings from this workshop will be documented to inform the development of security guidelines for the automotive sector.

Post Quantum Cryptography (Quantum-Resistant Cryptography)

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If cryptographically relevant quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. 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.

The NIST National Cybersecurity Center of Excellence (NCCoE) is collaborating with stakeholders in the public and private sectors to bring awareness to the challenges involved in migrating from the current set of public-key cryptographic algorithms to quantum-resistant cryptographic algorithms. The initial scope of this project includes engaging industry to demonstrate the use of automated discovery tools to identify instances of quantum-vulnerable public-key algorithm use and develop a migration plan that is prioritized based the criticality of the data. Another component of the project is to collaborate with the technology producers to perform interoperability and performance test of the implementations of the NIST standardized quantum-resistant cryptographic algorithms in products, services, and protocols.

Next Steps

Changes in these algorithms will significantly impact all sectors, including the development of AVs which are highly public key cryptography implemented in hardware and software. The industry will need to consider impacts during the traditionally long development timeframe for vehicle design. NIST is reaching out to the automotive sector (among others) to gather feedback on the development of tools and guidance for the implementation of these new algorithms. The Dioptra project is also looking for one or more partners within the AV community to help demonstrate the usefulness of the framework to the range of problems that are relevant to AV systems and to help identify what new features are needed to better enable Dioptra to address the research challenges.

Tentative Breakout Discussion Questions

- Are these valuable areas that NIST is concentrating on for cybersecurity of AV?
- What are other areas of cybersecurity in AVs that NIST should consider for research?

- Understanding that AI can be used to help improve safety, fuel efficiency, and other critical functions, it can also introduce cybersecurity risks. What would you say are the major cybersecurity risks and how can organizations determine the tradeoffs in the technology?
- While the focus of this workshop is on cybersecurity in AV, what are other areas in vehicle cybersecurity that you would suggest NIST to work on? Are there any other gaps in the vehicle cybersecurity?

Communications

Problem Statement

Connected and automated vehicles have significant potential to positively impact our lives and support economic growth. Advances in communications capabilities – for wired and wireless onboard vehicle networks and offboard communications with other vehicles, services, and infrastructure in the driving environment – can drive innovation in vehicle automation. The NIST AV research program has a key effort focused on AV communications[3] that includes evaluating the communications requirements for relevant driving scenarios, developing network modeling capabilities, and integrating the network models into a co-simulation (and ultimately the NIST AV Systems Interaction testbed) to evaluate integrated vehicle behavior including with respect to safety and AV communications perturbations.

AV communications include everything (V2X) from vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-network (V2N), and vehicle-to-pedestrians (V2P), and involve multiple communications protocols such as cellular C-V2X, 5G New Radio (NR), and the (older) dedicated short-range communications (DSRC). With improved latency, range, and infrastructure availability in the future, AV communications will play an increasing role to support ADS and features that will rely on information and signals sent through networks to augment on-vehicle sensors and intelligence (in current AVs). NIST can provide metrology to improve understanding of AV communications and how it could be utilized by vehicles in major challenge areas, such as:

- What information must be exchanged to realize an automated function in each context
- How information should be exchanged and processed to ensure timeliness and security without overloading the AV (and its connected networks) with too much information
- Classification and characterization of factors in the driving environment (described by NIST's Operating Envelope Specification[4]) that can impact information exchange with the AV
- Test metrics and methods to assess the performance of the AV communication network(s)

What NIST has Done

A simulation-oriented approach to AV communications is adopted to address these challenges. The advantages of simulation over on-road testing are that it allows for targeted and reproducible experiments to test scenarios of interest, and it can cover, with low risk and low cost, the many failure cases that would impact people or the surrounding environment. However, pure network simulation does not provide an accurate representation of vehicle dynamics or the physical environment, and it must be combined with models of those domains. This can be done either offline using data from sources such as naturalist driving data, or online through integration of hardware and simulators dedicated to different domains or sub-systems into a co-simulation. The co-simulation approach is used for NIST AV efforts due to the potential to replace one or more simulated systems with physical hardware, such as a vehicle with a complete automated driving stack. Ultimately on-road AV testing including AV communications is required to validate safety, performance, and trustworthiness of AVs.

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-

[3] https://www.nist.gov/programs-projects/automated-vehicles-and-av-communications
[4] https://www.nist.gov/publications/automated-driving-system-safety-measurement-part-1-operating-envelope-specification

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 are developed to simulate 5G NR cellular networks and V2X communications and incorporate fundamental PHY-MAC NR features aligned with 3GPP NR Release 16 and complying with scenarios and channel models based on 3GPP TR 38.885.

With safety as the top priority in mind and by noticing that lead vehicle deceleration is one leading crash-imminent scenario (SAE J2945/1), the use case Emergency Electronic Brake Lights (EEBL) is selected as the initial case to study the role of AV communications in reducing crash risks. A ns-3 scenario is developed with three vehicles in the same lane, where the lead vehicle broadcasts a Basic Safety Message (BSM) upon a hard-braking maneuver, and the following vehicles act accordingly upon BSM receptions. 5G NR sidelink with required functionalities is implemented for BSM transmissions, where its configurations and transmission parameters are adopted from the LTE parameter settings per SAE J3161/1 and after an in-house exercise on LTE-NR parameter mappings. The developed ns-3 scenario is further validated by initial data collection and analysis. A visual demo using NetSimulyzer shows the resulting trajectories of the three vehicles, which vary based on vehicle speed, distance, processing delay, and communication settings. A more comprehensive sensitivity study is in progress with the goal of extracting key factors and gain insights into using AV communications to reduce crash risks.

These network simulation capabilities are being incorporated into the broader NIST SERI effort through integration of ns-3 into the systems interaction testbed under development. As part of this effort, a new ns-3 module was developed that enables the network simulator to exchange data and synchronize its execution with external processes. This module was used to integrate ns-3 with the Robot Operating System (ROS) enabling co-simulations through ROS with automated vehicle simulators such as Simulink and CARLA. Additional collaborative efforts include evaluating impact of cybersecurity on latency of AV communications (IEEE 1609.2), supporting the development of teleoperations guidelines (Teleoperations Consortium), and leading the NIST Automated Driving Systems Technical Working Group (ADS TWG).

Next Steps

Future work will include continued integration of AV communications into the NIST systems interaction testbed, both in co-simulation and eventually hardware-in-the-loop, and applications of the testbed to AV communications use cases including interactions between AVs and infrastructure. Continued development of AV simulation capabilities and network models will enable study of the effects of realistic perturbations on communications (and other, e.g., sensing and perception) systems. These perturbations include interferences in the physical and electromagnetic environments.

Tentative Breakout Discussion Questions

- Are the topics and challenges that NIST is currently focused on likely to address important technical problems and/or accelerate AV deployment? What can NIST do in AV communications to have the most impact?
- Are there other organizations that are working in this area (AV communications) that NIST should coordinate with?
- What is currently inhibiting adoption of AV communications? (examples: slow government mandates, latency requirements, infrastructure availability, lack of spectrum)
- What are some of the measurement and standards challenges facing AV communications?

- What is your prioritization of the different V2X protocols for short, mid, and/or long-range AV communications systems, and why? (examples: C-V2X, 5G, DRSC, WiFi)
- What approach should be employed for testing AV communications?
- What AV communications scenarios are particularly important to evaluate?
- Is there additional AV communications R&D that should be conducted to address technical/measurement challenges?

Artificial Intelligence

Problem Statement

AVs are increasingly relying on AI for their operations. Currently, all commercial AV systems use the modular approach, where each component has separate models for each of perception, localization, planning, and controlling. AI components used in modular AV system include sensor data collection and sensor fusion, perception and object detection, Simultaneous Localization and Mapping (SLAM), and path planning and decision-making. Therefore, AI components must meet the following requirements:

- *Safety and redundancy:* Safety is paramount in AVs. The AI system must be designed with redundancy in mind, ensuring that there are backup systems in case of failures and that the vehicle can handle unexpected situations safely.
- *Regulatory compliance:* AVs must adhere to strict regulatory standards. The AI system needs to be tested to meet these standards and ensure compliance with relevant laws and regulations.
- *Continuous learning and updates:* AVs can benefit from continuous learning and regular software updates to improve performance, address new challenges, and stay up-to-date with the latest advancements in AI.
- *Human-machine interface:* The AI system should be able to communicate effectively with passengers or human operators, providing information about the vehicle's status, intentions, and potential safety concerns.

Estimating Uncertainty in Machine Learning (ML) Models in AVs

An epistemic uncertainty, also known as systematic uncertainty, refers to deficiencies caused by a lack of knowledge or information. While epistemic uncertainty can be reduced by increasing the amount of representative training data, it cannot be fully eliminated. Aleatoric uncertainty, also known as statistical uncertainty, refers to unknowns that differ each time we run the same experiment. Because the atmosphere is a chaotic system, atmospheric events impacting the road conditions where the AV operates are a source of aleatoric uncertainty. Consequently, even the best model trained on this data will not be able to provide a definite answer.

Generally, uncertainty estimation has been addressed by estimating the probability distribution associated with an ML task. For example, a ML classification problem involves predicting a label for a given instance; the same problem with uncertainty estimation involves predicting the *distribution* of labels. For large deep learning models and datasets, this process requires novel estimation techniques including deep ensembles and Bayesian neural networks. The intuition behind deep ensembles is that training with many randomized instances of the same neural network is like sampling from the distribution of best-possible neural networks. Bayesian neural networks, on the other hand, explicitly model the desired probability distribution. This is done by imposing a prior distribution over the weights of the neural network, and then approximating the corresponding posterior distribution following Bayes' rule. These approaches have tradeoffs regarding the quality of the uncertainty estimates, as well as the amount of computing needed. It is an open question as to what uncertainty estimation approach works best in the AV setting.

Computing Resources in AVs

One of the major factors is the lack of computing resources in an AV, since computation is limited to local hardware. Furthermore, since the vehicle must interact with the environment in real-time, the time interval for decision-making is very small. Another challenge is the data quality and

quantity. Real-world data comes with caveats like occlusion due to environmental conditions or due to partial visibility, that can hamper performance of deep learning models. In real-world scenarios, interaction between an AV and the entities on the road can encounter edge cases absent from the training data. Dealing with edge cases is not a trivial task and is directly associated with the robustness and resilience of the deep learning model. The widely used methodology of data collection by vehicle-mounted cameras can lead to an excess of uneventful data, which can further restrict generalization of the model during training. Alternatively, an AV may be equipped with several sensors that regularly collect, discretize, and process data to feed into the ML models. These sensors have inherent uncertainties that enter the deep learning model as aleatoric uncertainty, and quantifying and associating an uncertainty with an outcome is a difficult task.

What NIST Has Done

Development of a Taxonomy of Attacks and Mitigations in Adversarial Machine Learning

The NIST AI 100-2 report on artificial intelligence (AI) develops a taxonomy of attacks and mitigations and defines terminology in the field of adversarial machine learning (AML). Taken together, the taxonomy and terminology are meant to inform other standards and future practice guides for assessing and managing the security of AI systems by establishing a common language for understanding the rapidly developing AML landscape. Future updates to the report will likely be released as attacks, mitigations, and terminology evolve.

Development of Dioptra for the Automotive Community

Aligned with the Cybersecurity thrust, NIST has developed Dioptra for stakeholders from the automotive community. The Dioptra testbed is specifically focused on adversarial attacks against ML algorithms in AVs and defensive strategies. While there are a large variety of types of ML attacks for AVs, 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 will influence uncertainty. Data Description Object (DDO) format and a Data Interrogation Sheet (DIS) To manage uncertainty and risk in AVs, specific requirements to support standards and manage risk for AI use are required. By extending NIST's AI Risk Management Framework, NIST has drafted a DDO format and a DIS. By providing a standardized DDO format, simulations and ML models can be appropriately described for evaluation. The DIS can be used to access the DDO format by external stakeholders.

Next Steps

NIST will finalize NIST AI-100-2e2023 and continue to maintain it on an annual basis. NIST will also work to develop recommendations for improving the robustness and mechanisms for technical evaluation of object detection and classification in AI perception systems used in vehicle ADS and ADAS. NIST will finalize the AV DDO format and DIS for AV stakeholders. In addition, NIST will further tailor and promote Dioptra to the AV community. Alongside the other AV thrusts, NIST will integrate its AI efforts with hardware-in-the-loop capabilities to further advance the development of safe and secure AI in AVs.

Tentative Breakout Discussion Questions

- What are the top challenges related to uncertainties in object detection and classification by vehicle computer vision systems for autonomous driving?
- What challenges exist in AI deep learning technologies that can significantly impact the robustness and efficiency of computer vision perception algorithms?
- What deep learning models are available for object classification in AV and how could they be augmented with uncertainty estimation for use in driving scenarios to assess their impact on these challenges?
- How can these technologies be characterized and validated for those solutions?
- What standardization efforts, if any, are required to accelerate the deployment of these technologies?

Accelerating the Deployment of Digital Infrastructure for Roadway Safety

Problem Statement

According to NHTSA, a tragic 42,795 deaths and millions of accidents occurred on US roads in 2022.[5] Speeding, wrong-way driving, unprotected lefts, and more driver behaviors and driving scenarios unnecessarily kill drivers, passengers, vulnerable road users (VRUs)[6], and others. Digital infrastructure, defined as all roadway technology assets that create, exchange, or use data or information in a digital form as a part of their operation[7], offers safety solutions now for crashes involving human-drive vehicles. Further safety gains can be realized through AVs whose deployment can also be enabled by digital infrastructure.

OEMs are investing heavily in the development of vehicles and technology across applications including personal vehicles, trucking, transit, ride hailing, and delivery vehicles. ADS are designed to completely replace human drivers in AVs; while ADS deployment is advancing, the deployment is far from a level that will significantly reduce mortality. Digital and physical infrastructure can enable deployment across operating design domains (ODDs) and vehicle types. Meanwhile, active safety features and SAE Level 1-2 driving automation features are increasingly prevalent in today's vehicle fleets and are intended to improve safety and convenience for human drivers.

While extensive deployment of AVs is unpredictable and unlikely for decades, Infrastructure Owner-Operators (IOOs) can significantly improve roadway safety in the near term by focusing on digital infrastructure that supports human driver and VRU safety. Such investments will increase overall safety as well as pave the way for the introduction of AVs. The situational awareness and connectivity that such investments will provide will be of high value to AVs, offloading processing they need to implement, allowing them to achieve the competence their ADS require earlier.

The possible, near-term safety outcome improvements that digital infrastructure can address include critical scenarios such as VRU safety, especially at intersections, work zone safety, weather-related hazards, and wrong-way drivers. Solutions include traffic signal digitalization, V2I communications, AI applications to traffic operations centers, and more. Public and private IOOs need support in identifying and prioritizing effective use cases and validated implementation solutions. Though research has been done on safety uses cases and digital infrastructure, information has not been compiled and published in a form that is readily accessible to IOOs. A standard template for the definition and publishing of use cases is required along with a parallel mechanism for the publication of proven use case solutions. A national initiative to inventory and make use cases available in a standard, verified form can provide IOOs with the data they require to prioritize investments plans.

[5] https://www.nhtsa.gov/press-releases/traffic-crash-death-estimates-2022
[6] VRUs include pedestrians, cyclists, e-scooter riders, wheelchair users, etc.
[7] https://www.toronto.ca/city-government/accountability-operations-customer-service/long-term-vision-plans-and-strategies/smart-cityto/digital-infrastructure-strategic-framework/

NIST's Role

NIST proposes an appropriate, national organization develop a use-case template to drive a community-wide collection/definition of use cases and proven solutions across the USA. Further, to accelerate the development and implementation of solutions for use cases, some basic engineering support is required. In particular, the operational capabilities and characteristics of available technology need to be measured and published so that developers/implementers know which particular technology instantiations they should deploy. We propose that NIST collect these data and work with the aforementioned national organization to publish it.

Tentative Session Discussion Questions

- What are the top safety issues, such as work-zones, intersections, VRU, wrong-way drivers, excessive speed, etc., that can be addressed by digital infrastructure (V2X)?
- What enabling infrastructure technologies in LIDAR, RADAR, camera, and AI that are available?
- How could we accelerate the deployment of digital infrastructure applications/technologies?
- How can digital infrastructure technologies be characterized and validated for those use-cases?
- What standardization efforts, if any, are required to accelerate the deployment of these technologies? What are the barriers to this standardization and deployment of these technologies?
- What do IOOs need to implement into this technology?
- How can we build or enhance a national database of infrastructure use-cases and solutions?