NIST Standards and Performance Metrics for On-Road Autonomous Vehicles Workshop Summary

1. Introduction

This section provides background context behind the National Institute of Standards and Technology (NIST) effort to advance the state of on-road autonomous vehicles in addition to the purpose for the Performance Metrics for On-Road Autonomous Vehicles Workshop held virtually on March 8th and 9th 2022.

a. Background

On-road autonomous vehicles are projected to influence key aspects of everyday life including transportation, goods delivery, manufacturing, public safety, and security. However, on-road autonomous vehicles can pose a risk in the event of unexpected system performance. In addition, the autonomous vehicle sector is a vastly inter-disciplinary field with subject areas including perception, planning, control, safety, cybersecurity, and communications. Furthermore, autonomous vehicles can pose a risk in the event of unexpected system performance. Therefore, industry and government agencies are looking to NIST to characterize the performance of these complex systems to mitigate risk to both the manufacturers as well as the consumers.

b. Workshop Goals

NIST is a nonregulatory government agency under the Department of Commerce that is equipped to develop test methods, metrics, and standards to characterize the performance of these complex systems. Therefore, NIST is currently determining focus areas of interest to characterize the performance of autonomous vehicles to mitigate risk to manufacturers as well as consumers.

This workshop was aimed to solicit stakeholder feedback to identify key areas where NIST could develop standards and performance metrics to help advance the on-road autonomous vehicle field. In addition, this workshop was aimed on fostering a multidisciplinary community consisting of stakeholders from a variety of disciplines and domains in autonomous vehicles. This workshop was part of a larger effort by NIST to convene industry experts in the on-road autonomous vehicle space and reduce barriers to entry and innovation within the market.

To achieve those goals, NIST invited keynote speakers to introduce the important topics of the workshop. Furthermore, NIST invited multidisciplinary panelists from government, academia, and the private sector to participate in focused panel discussions. Finally, the workshop included facilitated breakout sessions which allowed participants to offer feedback in the key topic areas.

2. Keynote Speeches and Panels

This section discussed the relevant topics heard from prominent government officials and domain experts. The audience interaction in the keynote speeches and panels were limited to asynchronous Q&A because the primary audience interaction was reserved for the breakout sessions. A total of five one-hour panels were held in the following focus areas: safety, communications, cybersecurity & privacy, artificial intelligence, and sensor perception.

a. Introductory Remarks and Keynote Speeches

At the beginning of each day, introductory remarks and keynote speeches were provided. These presentations were given to level set and inspire discussion for the following workshop elements. Presentations were given by the following:

- **James K. Olthoff**, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director (Currently Associate Director for Laboratory Programs), National Institute of Standards and Technology

Dr. Olthoff described NIST's role in establishing standards and emerging technologies. He recognized the vast interdisciplinary field of the autonomous vehicles sector, and the many factors that the sector relates to including perception, planning, control, safety, cybersecurity, and communications. He noted the difficulty of identifying of another technology that touches so many elements of NIST's portfolio. Autonomous vehicles bring great benefits but also risks, so their system performance needs to be sound and secure. He noted that developing the required level of trust for such vehicles requires standards and measurements, and therefore well-suited to NIST's mission. He described NIST's previous history in the field since at least 2004 and remarked on the progress in the years since. Finally, Dr. Olthoff thanked the attendees for their participation and for bringing their perspectives and experience. Together, he challenged the workshop to help build confidence that autonomous vehicles will behave safely, securely, and appropriately, thus developing the trust in that technology that the public needs.

- **Nell Abernathy**, Director Office of Policy and Strategic Planning, Department of Commerce

Mrs. Abernathy shared her pleasure in representing the Department of Commerce and shared some of the agency's priorities of broadly shared prosperity, domestic innovation, investments in the industrial base, international collaboration. The mission is to support these advancements and innovation, and she reminded attendees that we will be unable to succeed in the 21st century unless we are able to harness the talents of all Americans and all communities. As we facilitate and expedite the development and commercialization of emerging technologies, we recognize the need to promote collaboration among federal, state, local, tribal, territorial, business, not-for-profit, and academic institutions. As a champion of advancing standards and developing measurement science solutions to challenging technical problems, NIST is well positioned to represent the federal government, drawing upon NIST's experience in areas such as AI, cybersecurity, and materials- and physics-based technology. She described the focus areas for the workshop as we aim to continue U.S. leadership in promoting an open dialogue in promoting on-road autonomous vehicle development. On behalf of the Secretary of Commerce, she thanked attendees for their participation and for their past, current, and future progress.

- **Trent Victor**, Director of Safety Research and Best Practices, Waymo

Dr. Victor is an employee of Waymo, which is currently developing robot-taxis. His keynote speech was subject to proprietary information protection during this presentation.

- **Tim Kurth**, Chief Counsel (R), United States House of Representatives, Energy and Commerce Committee Consumer Protection and Commerce Subcommittee

Mr. Kurth welcomed attendees to Day 2. He described the importance of standards and performance metrics that will be supported by NIST and the National Highway Traffic Safety

Administration (NHTSA) as on-road autonomous vehicles move to commercialization. He described the benefits that on-road autonomous vehicles will provide as a new form of mobility. He shared the risks of inaction, for example, noting that Department of Transportation 2020 figures reflected more than 38,000 fatalities in crashes nationwide – a statistic that the U.S. hopes will be greatly diminished by on-road autonomous vehicles. Mr. Kurth described legislation supporting NIST work on national strategies, through the Department of Commerce, in the areas of artificial intelligence, Internet of Things, advanced manufacturing, quantum computing, blockchain technology, new and advanced materials, unmanned delivery services, and three-dimensional printing. He advocated for progress on a national privacy and data security framework.

- **Adam Campbell**, Senior Manager Safety Innovation and Impact, Gatik

Dr. Campbell introduced Gatik as an organization that currently uses autonomous vehicles for logistics and deliveries. He opened the discussion with a hypothetical question about how one should react when an autonomous vehicle is involved in a collision that a human driver would have avoided. He proposed that an autonomous vehicle should perform at least as well as a human, thus establishing human driver performance as a baseline. He reminded attendees that innovative changes have occurred in the past, illustrated by the difference between 1900 and 1913 where horse-drawn carriages gave way to automobiles. He noted that technology often precedes policy, but that good teams working together help to progress to safer, more reliable solutions. We have successfully confronted challenges of this significance before. Drawing on discussions from Day 1, he reflected on some of the considerations that will go into that benchmarking and the need to look at ways to address challenges, including the difficulty of establishing metrics that will prove safety. Research demonstrates that it is difficult to perform a statistical comparison within existing drivers due to their sheer number and performance variation. Therefore, it may be beneficial to use a human benchmark as a consideration supporting system design and testing. Therefore, confidence and metrics can be provided if our resulting design and performance match those of a human being. He pointed out that industry can take advantage of research, such as studies performed by NHTSA, and that comparing our data and observations of our autonomous vehicles to these types of data will help set some benchmarks about what to expect and explain vehicle performance. He also shared that, if industry doesn't develop metrics to at least set the floor regarding expectations, then the courts will, and the consequences of lagging could be significant. He thanked participants again for their work and encouraged the attendees to continue their progress.

b. Panel Discussion: Safety

Moderator: Edward Griffor, National Institute of Standards and Technology
Panelists:
Chan Lieu, Aurora
Edward Straub, SAE
Jack Weast, Intel
Bert Kaufman, Zoox
Robert Dingli, Plus
Robyn Robertson, Traffic Injury Research Foundation

The panelists began by discussing the biggest challenges facing on-road autonomous vehicle safety. Some of these challenges were technical, others were non-technical. A significant non-technical challenge is convincing the public that vehicles are safe while a significant technical challenge is interacting with other road users. Predicting human behavior is difficult and will rely on advancement of computation. Within these technical and non-technical challenges, the panelists discussed the notion of how to create a "safe system" while accommodating various use cases.

Panelists agreed, there is no such thing as perfect safety since the act of driving is inherently risky. Therefore, the panelists posed questions back to the group:

- How do we know the vehicle is safe enough to deploy?
- What is an acceptable level of safety?
- Who sets the acceptable level of risk?
- How do we go about incorporating different factors in our requirements?

The panelists then turned to the question of defining standards and performance metrics. The discussion continued to explore defining safety in given scenarios. Panelists highlighted the unbounded number of potential scenarios that could be created and tested. The challenge with a scenario-based approach is the constantly changing landscape and additions of new scenarios. A set of known scenarios would be a place to start but would need to be updated and pushed consistently. A finite set of use-cases could be utilized during the development process. The aim would be that the case set is sufficiently large to demonstrate reasonable safety while recognizing there are edge cases which are untested. If the operational design is enterprise scale, the data set would be very large and a barrier to entry for smaller organizations.

Another approach to defining safety would be to utilize a metrics-based approach. The panelists discussed the challenges of defining the right level of abstraction for metrics. Some metrics may be too general to be testable, some metrics may be too specific to be applicable to all situations. The panelists discussed the feasibility of separating testing metrics from scenarios to maintain safety standards while not inhibiting the development of the technology.

The panelists moved on to discuss the baseline environment of the autonomous vehicle and the effects of the environment on safety considerations. Panelists highlighted current considerations in their organizations including emergency vehicles, road conditions, pedestrians, infrastructure data, and other non-autonomous vehicles. While these considerations are important to the on-road autonomous vehicle safety, the panelists suggested a need to baseline expectations of safety from these environmental variables. There does not currently exist a standard vocabulary for discussing these variables and the corresponding expectations of safety. The panelists agreed that infrastructure changes (consistent roads, data on road work, road marking) would be helpful, and that those changes take a long time to implement and deliver value.

The panelists concluded the time by discussing human-machine interaction. Panelists highlighted the need for intuitive and responsive interface with the vehicle. While there are some use-cases where the vehicle is empty, the human remains a large part of the system. Therefore, the human in the vehicle and humans outside of the vehicle will affect the safety of the vehicle. There currently is no baseline of what to expect or make predictions of what the humans inside and outside the vehicle will do. With the number of variables inherent in the human-machine interaction, simulation was discussed a tool to reduce errors after deployment. Panelists agreed that a feedback loop of improvement was needed after deployment to continually raise the safety bar for autonomous vehicles.

c. Panel Discussion: Communications

Moderator: Scott McCormick, Teleoperation Consortium
Panelists:
John McNicol, British Standards Institute
Stan Schneider, Real-Time Innovations
Maarten Sierhuis, Nissan North America
Fan Bai, General Motors
Bettina Erdem, Continental Corporation

The panel first discussed the challenges and solutions to teleoperation. Generally, the panel agreed that teleoperation had many challenges that were focused on the interaction between the human and the machine. Being able to handle corner cases (construction zone, police interaction, rescue missions) is essential to the mass deployment of driverless cars. The vehicles already possess a tremendous amount of processing power; however, connectivity of the remote operator to the vehicle is a large hurdle. Panelists discussed the need for an ontology of teleoperation modes (time-sensitive and non-time-sensitive teleoperation). The panel suggested standards around the training and certification of the remote operators and remote operator stations as potentially useful.

The panel discussed the broader topic of communication technology. From a conceptual perspective, the panelists discussed the communication of a vehicle with another vehicle, the vehicle to the infrastructure, and the infrastructure to the vehicle. There are currently many different approaches to the communication of the system components. There is currently no standard data format, channel, or presentation layer for users. There is a need to directly share communication-focused data sets and not worry about language barriers.

A challenge to any communication approach will be the channel over which the communication is transmitted. The panelists discussed the use of many bandwidths for communication. Similarly, the panelists highlighted the challenge of 5G roll out in rural areas. Latency will be a challenge no matter which channels are used. The availability of timely and relevant data to any given vehicle will be important to maintaining safety.

The panel discussed long and short-range communication platforms and the need to create a holistic view of the world on the vehicle platform. The topic of sensor and perception fusion was discussed as a need for achieving the single world map view. The coordination, cooperation, and collaboration of multiple vehicles with different sensor load outs was generally agreed to a goal of this holistic view. From this single view, a “democratization of safety” could be achieved on the road.

The panel also discussed the need for standards in the vehicle communication space. Panelist agreed that timing of standards is important. If a standard is too early, it stifles innovations, if it is too late, there is no market cohesion and progress. For autonomous vehicles, the panelists suggested a taxonomy of different environmental variables (speeds, road conditions, traffic data, and meta-data) that could be communicated between vehicles. There are communication standards for non-autonomous vehicles which could be extrapolated to on-road autonomous vehicles.

d. Panel Discussion: Cybersecurity & Privacy

Moderator: Katherine McClaskey, Cybersecurity and Infrastructure Security Agency
Panelists:
Adam Mistick, Ford
Anuja Sonalkar, Steer
Christos Papadopoulos, University of Memphis
Amie Stepanovich, Future of Privacy Forum

The panelists began by discussing the unique challenges to cybersecurity in the on-road autonomous vehicle domain. While confidentiality and integrity are important, panelists agreed that availability is the critical security principle to focus on. The panelists agreed that ensuring the vehicle is working as intended and available to the driver are the biggest concerns with cybersecurity.

As on-road autonomous vehicles become more sophisticated and add more features, the complexity of those systems increases. This complexity accelerates cybersecurity concerns as the communication between features and components on the vehicle are vulnerabilities for malicious attackers to target. The panel discussed threat scenarios in which the attackers sent fraudulent signals to the vehicle or caused a denial of service of a component. These scenarios could render the vehicle unsafe to drive and thus pose a significant risk to the driver and others on the road.

A common topic of discussion was supply chain considerations. The current disruption in microchip processing is affecting on-road autonomous vehicles the same way that it is affecting personal computers. These disruptions cause the same types of threats to on-road autonomous vehicles and thus must be addressed. Alternatively, the panelists suggested that the on-road autonomous vehicles are similar to other systems that exist today while also having custom hardware and software technology. There are inputs and outputs, therefore, some best practices and concepts can be leveraged or translated to the on-road autonomous vehicle space.

Finally, the panelists discussed privacy and trust. The end user is ultimately deciding on whether to trust the on-road autonomous vehicle and its capabilities. As the data collection of the on-road autonomous vehicle platform increases, the ability for the system to maintain privacy becomes more difficult. Giving users a way to make informed choices about their data while also maintaining their safety is a key balance to strike when constructing cybersecurity and privacy for autonomous vehicles.

e. Panel Discussion: Artificial Intelligence

Moderator: Elham Tabassi, NIST
Panelists:
Daniel Carruth, Mississippi State
Alberto Lacaze, Robotic Research
Hussein Mehanna, Cruise
Alfred Chen, University of California Irvine
Vijay Patnaik, Applied Intuition
Kevin Zaseck, Toyota Research Institute

Panelists highlighted important challenges facing the Artificial Intelligence (AI) community in on-road autonomous vehicles. Challenges ranged from trustworthiness, security, safety, and complexity. Currently, the public is having an open debate on the trustworthiness of on-road autonomous vehicles. This debate stems from issues surrounding the safety of the vehicles whether from errors in object detection, data processing, or malicious actors. The development of safety measures remains difficult due to the complexity of breaking those metrics down into component level measures and tests. The panelists suggested that more conversation is needed around these topics while best practices are being developed.

The panel then discussed the topic of testing AI systems. Panelists suggested the use of simulators has shown benefits before using human testing to raise acceptance rates. The panelists also highlighted the balance of coverage and resource utilization. While AI is a new tool, there are previous examples of safety critical industries (such as the airline industry) that have best practices surrounding tooling. The community could leverage those tools and techniques while not duplicating previous efforts. Concurrently, panelists suggested that testing AI in on-road autonomous vehicles be conducted continuously and transparently because sensors can decay, conditions can change, and algorithms can be updated. Therefore, all tests, along with their associated measures, should be monitored and communicated clearly.

The panelists turned their attention to the topic of AI safety. As with previous panels, the discussion centered around the dependency of safety on operational design domains (ODD). While a given scenario may be safe in one ODD, the same levels of safety will not suffice in another ODD. Flexibility in determining the context will be critical for AI safety. As a potential lens to view the challenge, the panel suggested a risk-based approach. Determining frequency and severity of a given incident or failure can be a way to assess risk and thus the mitigations and tests needed. While the panel agreed there was no such thing as a zero-risk solution, they also suggested that the mitigation must be less harmful than the original risk. Therefore, the panel suggested that AI systems should be able to determine when they are operating outside of risk parameters and take corrective actions based on a continuous feedback loop.

The panel also discussed the importance of data to AI solutions in autonomous vehicles. Panelists highlighted issues regarding data curation and data traceability. While the data within testing environments has produced positive results, the ability to trace issues back to the initial, incomplete data set remains a challenge. Other panelists discussed approaches for data acquisition. There are currently no standard approaches to acquiring, generating, or mining relevant data for most use cases. Concurrently, when dealing with large data sets, the underlying distribution of the data may appear to be normal, however, the algorithm is biased against a certain outcome or demographic. Understanding bias in the data, and thus the AI, is important to consider when deploying autonomous vehicle systems.

f. Panel Discussion: Sensor Perception

Moderator: Kamel Saidi, NIST
Panelists:
William Buller, Michigan Tech Research Institute
Rajeev Thakur, Velodyne
Brent Fisher, Auto Lidar Expert
Ryan Lamm, Southwest Research Institute
Zeb Barber, Aurora

Panelists discussed the challenges facing the sensor market in on-road autonomous vehicles. They highlighted the fact that there are many uncoordinated vendors. Each sensor defines their own metrics for reporting targets and physical measures. This lack of standard vocabulary on metrics leads to point-to-point decisions between vendors and original equipment manufacturers (OEMs) which increases the resourcing needed to compete in the standard market. Similarly, overall vehicle system requirements are not standardized. This lack of definition results in scattered sensor requirements and increases complexity for developing automotive solutions.

The panel also discussed the importance of the ODD in developing sensors. Currently a bottom-up approach is used where sensors are built and combined to create an ODD. Panelists suggested creating a standard definition of an ODD to provide a top-down approach. This approach would create valid use-cases for sensor fusion to achieve a specific mission. Panelists also commented that a common definition would allow for the industry to address gaps in current sensor technology by identifying the capabilities that are not present instead of assuming more of the same will solve the problem.

The panelists discussed benchmarks for sensors. Current practice is for OEMs to solicit an Request for Quote (RFQ) and attempt to find best quote from the responses. This type of activity is driving development around specific challenges and the language of a given organization and not challenges that may be present across the market. The panelists suggested that creating benchmarks for both sensor level metrics (target size, target detection, number of pixels on target, framerate, etc.) and algorithm level (sensor agnostic) metrics could be beneficial to standardizing the space. Additionally, the panel suggested that standardizing the vocabulary of the processing space would be helpful (perception, computation, actuation, etc.).

The panel also discussed the different issues of operating within the test range versus the real world. There are many variables that are present in deployment which are not accounted for in the lab, sometimes referred to as ‘confusers’ to a perception system. The panel provided many examples of these variables (road conditions, signal lights, signs, environmental conditions). These variables, even when considered, do not have standard definitions nor the ability to determine suboptimal values. The panel suggested that defining these variables and determining ranges for those variables would be helpful to increasing repeatability and reliability of sensor systems.

The panel discussed sensor fusion. Panelists highlighted the balance between approaching sensor fusion from a hardware or software perspective. In the past, hardware was more expensive and computing power was difficult to acquire; this led to more simple and elegant solutions in the software space. Conversely, hardware and computing power is more readily available to organizations and thus the constraints on software have relaxed. As the volume of data increases, the panelists suggested creating latency metrics and sensor fusion metrics to appropriately incentivize hardware and software development.

3. Breakout Room Discussions

Breakout room discussions were conducted to solicit feedback on focus areas with respect to performance testing and standards in on-road autonomous vehicles through active audience participation. Each breakout room was facilitated by at least one professional moderator and were conducted through two one and a half hour sessions.

a. Safety

During the discussion, participants highlighted that safety was the top concern when considering autonomous vehicles. Given its importance, participants suggested It would be helpful for NIST to work with other agencies to develop appropriate safety risks. In addition, NIST could help define an appropriate level of risk which is a baseline for all autonomous vehicles. Participants also provided that acceptable risk is dependent on a given context and that a challenge will be determining a common set of risks.

Participants also focused on the concept of testing safety requirements. Participants discussed the distinction between the relative challenges for test requirements for at fault crashes versus not at fault crashes. The discussion did not reach any concrete conclusions. Participants discussed the potential to shift the safety question to examine the context of a situation to determine risk requirements.

While there is not sufficient knowledge to define a test that would determine a vehicle is safe or not, any tests that are defined should include parameters for the random events that can occur within the environment of an autonomous vehicle. Given the wide range of parameters which could be defined, some participants suggested there was no credible test that can be designed to quantity safety in any meaningful way. To accommodate this gap, there is a need to think about the use-case of the technology when thinking about the test to deploy. This approach could produce reference scenarios, and metrics, which are tied to use cases. If this approach is taken, use-cases could be selected by organizations, thus rendering the one-size-fits-all standard as negligible. While this outcome is not ideal, participants agreed, having a baseline standard would be beneficial compared no standards.

Ultimately, participants highlighted that the guiding metric of safety is consumer trust. There could be tremendous value in the use-cases, tests, reference documentation, and metrics and that these approaches would be wasted work if the results were not communicated clearly to the public. Participants suggested any approach taken by NIST should include a public outreach and communications component.

b. Communication

Participants began by discussing the different type of communication networks that exist (Wi-Fi, satellite, dedicated short-range communications, cellular, etc.). This discussion centered around the requirements of those networks for communication between the vehicle and the environment around it. Many participants mentioned performance requirements for networked communication (teleoperation, latency, processing time, etc.). Examples of work done both domestically and internationally with integrating different types of networks into a cohesive system were discussed.

The conversation turned towards the overall ecosystem of communications that will need to occur to ensure on-road autonomous vehicles are providing as much functionality as possible. Participants mentioned the need for standards to normalize communication patterns within the vehicle, between the vehicle and infrastructure, and between the vehicle and the environment. Similarly, participants suggested providing ways for technology providers to integrate their systems together using communication protocols. As more stakeholders are added to the growing ecosystem of on-road autonomous vehicle communication, the need for a common language grows. Participants highlighted the need for business and use-cases to be developed so organizations can see value in the standards.

Participants then shifted the discussion to data fusion. Many participants highlighted the challenges of the location of the processing. There are multiple approaches to data fusion (centralized, de-centralized, distributed, hierarchical, hybrid) and selecting one or standardizing on such an approach is difficult due to the varied nature of use cases. Participants highlighted the need for a common language around the confidence and quality of data coming from a given sensor. It was agreed that a common world view for each vehicle is desired and therefore sensor and data fusion require standardized metadata at multiple levels of aggregation (sensor, vehicle, environment, infrastructure, etc.).

Participants moved on to discussing the security of the communications of an on-road autonomous vehicle. Given the connected nature of on-road autonomous vehicles, participants raised concerns over malicious actors taking over legitimate teleoperation of the vehicle. Additionally, participants discussed unintended behavior within normal operating conditions, such as platooning and lemming effects. It was agreed that security of communications was an open question and warranted further conversation.

c. Cybersecurity & Privacy

The discussions identified numerous areas where NIST can assist with on-road autonomous vehicle considerations in both the research side and with the development of standards and best practices. The attendees recognized that there are cybersecurity elements in all aspects of on-road autonomous vehicles. The community can build upon and adapt many existing models, such as vulnerability assessments, software/code evaluation, and advances in integrated DevSecOps methods. The complexity of on-road autonomous vehicles may prevent many of the current solutions from being directly applicable, so much work remains to adapt existing guidance for this emerging technology.

One element that needs further research is the risk imposed by after-market changes. Even if detailed and stringent security models are imposed at the manufacturing stage, there are postdelivery factors (unauthorized modifications, physical threats to street signs and other markers) that must be considered. As with more general cybersecurity considerations, supply chain provisions must be included in the on-road autonomous vehicles research and standards. The integrity of software and components is a critical factor.

Attendees pointed out that the life cycle of a vehicle is quite different from many other types of technology. Product cycles in traditional IT are short, while a vehicle may be expected to be operation for many years. Therefore, the longer cycle heightens the need for stringent and visionary planning. Furthermore, cryptography for securing internal and extra-vehicular communications will be a key consideration, possibly to include innovations in quantum computing. Processes for patching and updates will be a vital concern that must be consistently and reliably addressed. The community will also need to consider security implications for critical traffic infrastructure such as signage and intra-vehicle communications.

Breakout participants agreed that standards and guidance might include cybersecurity elements of roadworthiness criteria, possibly to include software currency elements, resilience considerations (how to address a loss of communications or a failed or attacked component), and domain-specific considerations (i.e., criteria for a passenger vehicle will be different from those for a truck hauling hazardous materials). These standards are likely to be regionally/geographically influenced.

A final element of the breakout session concerned privacy considerations. Participants agreed that a significant amount of data will be exchanged through the operation of on-road autonomous vehicles, and there will be concerns about what personal and private information is collected and monitored. This consideration represents an area where NIST may be able to provide some guidance, such as by recommending methods for opting in and what tiers of privacy data might be included. That guidance may consider privacy data ownership and discussion about who owns the data that describes where drivers have travelled and how the vehicle has been operated.

d. Artificial Intelligence

In the AI discussion, participants discussed both the general needs of the community for addressing risks to/from on-road autonomous vehicles and specific activities that NIST may be able to support. The initial conversation related to testing methods, including those for AI algorithms supporting vehicles. Because there are many differing contexts for different types of on-road autonomous vehicles, there is not a single set of tests that would fit all scenarios. Attendees felt though, that NIST (and the standards community, in general) may be able to develop test scenarios for specific ODDs. Attendees also noted that, because test conditions change, such as when sensors' performance degrade, any algorithms or test criteria developed must be adaptive enough to compensate for real-world conditions.

Participants expressed that, as with other areas such as cybersecurity and privacy, NIST is well-suited to provide measurement standards but may not be an appropriate party to apply those measures nor to define acceptability criteria. NIST can help define the concept of conducting testing, including the units to be measured, and algorithms, methods, and models that may be applicable for a given domain. Acceptability criteria might eventually be produced by legislators, insurance companies, and risk assessors.

The group agreed that a valuable contribution from NIST would be to provide consistent and standard terminology for the on-road autonomous vehicle industry. Many terms (transparency, explainability, predictability) are used in the industry but need more consistent definition. A common language is needed to support tools, techniques, and other criteria. Attendees felt that system designers and developers need actionable guidance. While the community has discussed many points of focus for decades, it is most helpful when guidance can be clearly understood and describe specific technical actions. Notably, there was a comment that safety and security are not the same, and even definition of those terms (and the difference between them) needs to be developed for this sector.

As discussion continued, attendees recognized that testing and information sharing may be hampered by the fact that systems, algorithms, and even previous results include proprietary data. There are also many layers of data – the actual vehicle engineering components may have an operational context, but there are AI aspects that may be distinct. Even if a product is certified as "secure" or "safe", there would need to be mechanisms for ensuring that no changes to the system might result in degraded safety or reliability.

At the close of the discussion, it was agreed that there is value in NIST assisting with definitions, glossaries, and test cases for common scenarios (for components, sub-components, and individual elements) that could provide better consistency in secure development and operation of on-road autonomous vehicles.

e. Sensor Perception

The breakout session began with a discussion on the challenges facing the space. These challenges included the volume, velocity, and veracity of the data being generated by the sensors. Specifically, participants highlighted the need for standards in the sensor data space to develop metrics on data quality. Additionally, participants noted that these types of standards would aid in the ability for upstream processing to make better decisions.

Participants considered the topic of LIDAR in on-road autonomous vehicles. Challenges were presented including no baseline of data, multiple sources of data, and no standardized return rate. Participants were split as to the necessity of LIDAR in every on-road autonomous vehicle. If a standard is desired in the LIDAR space, participants suggested collaborating with industry to align standards across the entire space as well as determining definitions and performance requirements.

Participants discussed the distributed nature of computing within an on-road autonomous vehicle. There are multiple sensors on a vehicle computing their sensor specific data and feeding the answers to compartmentalized processes to make decisions. This approach results in a lack of transparency when a failure occurs. Some participants noted that a lack of transparency also exists in specifications for sensors. As a solution, participants suggested creating sensor standards, complete with definitions and performance metrics, to alleviate the transparency issue.

From a market perspective, participants discussed the current sensor integration process. Currently, testing and integration onto a vehicle is done in a custom build for each project, with little to no commonality between projects. There was disagreement between participants if interchangeability of sensors, data systems, or processing was possible. Some participants suggested common testing mechanisms to provide common language on object definition, object detection, environmental variables, and functionality of sensors and perception.

f. Overarching Themes

During the panels and breakout sessions of the workshop, the NIST team identified the following prevalent themes.

While the concept of on-road autonomous vehicle safety had its own track, many participants highlighted the notion that safety requirements would drive the other track's outcomes. This top-down conceptual organization requires that safety requirements be considered first and used as input into the other concept's workstreams.

Many participants across the sessions highlighted the need for performance requirements. These requirements were intended to be as specific as possible such as within the sensors and perception session, defining wavelengths of light and luminosity thresholds and within the safety session, defining metrics which could be used to measure safety other than miles driven. These performance requirements were not necessarily the same for each track but rather consistent in the desire for them to exist.

Within a few tracks, the concept of fusion was discussed. Whether it was sensor, data, or contact fusion, participants highlighted the need to tackle the challenge of aggregating, aligning, and determining if multiple data points represent the same real object. Participants provided multiple approaches to this challenge: distributed, centralized, mesh, etc. No matter the approach, creating reliable sensor fusion aids in achieving a holistic, "one world view", of the environment.

Finally, participants recognized that any efforts in the on-road autonomous vehicle space should be collaborative. Participants suggested multiple government and non-government organizations that would be appropriate partners for NIST to engage during its work. NIST is committed to a public-private partnership model that seeks to achieve common understanding of the challenges ahead and the work to be done.

4. Next Steps

NIST would like to thank all participants, panelists, moderators, facilitators, and scribes for their valuable contributions to the workshop. Based on these contributions, NIST will take the comments provided and begin to draft a plan for work to be done in the future. Please check back in with the program at our website https://www.nist.gov/programs-projects/nist-and-autonomous-vehicles to receive updates on next steps.

NIST is always open to feedback. Please email questions, comments, or suggestions to the following email address: autonomousvehicles@nist.gov.