Wisconsin Automated Vehicle External (WAVE) Advisory Committee
Meeting Minutes

April 5, 2023 - 9:00am-1:00pm
- Meeting Held Via Video Teleconference -

Attendance

WAVE Members Present: Ray Mandli, Sia prosper, Adonica Randal, Alexander Pendleton, Art Harrington, Chris Hiebert, Debby Jackson, Jeff Lewandowski, Luke Junk, Maggie McNamara, Nick Jarmusz, Nick Musson, Evan Umpir, Patrick Vander Sanden, Rep. Dave Considine, Rick Lucero, Sen Jeff Smith, Steve Caya, Xiao (Shaw) Qin, Yang Tao, David Noyce.

WAVE-Member Organization Proxies Present: Eric Nutt (WiACES, GTiMA, Mandli Comm), Ellie Thorman (Staff of Senator Smith), Andi Bill (UW-TOPS Lab), Dan Johnson (WMCA), Edwin Rothrock (Chippewa-Eau Claire MPO), Nick Perna (FHWA)

Wisconsin Department of Transportation (WisDOT) Staff Present: Hannah Brown, Ethan Severson, Brad Basten, Alex McMurtry, Anne Reshadi, Brian Elliot, David Pabst, Diane Gurtner, Jessica Wagner, Joel Nilsestuen, June Coleman, Mike Kessenich, Kaleb Vander Wiele, Kyle Hemp, Lea Collins – Worachek, Maryne Taute, Matt Umhoefer, Paul Hammer, Rebecca Szymkowski, Reed McGinn, Rodney Saunders Jr, Ryan Spaight, Stephanie Arduini, Tracy Drager, Michael Denruiter

Meeting discussion

Welcome and Opening Remarks - WisDOT Secretary, Craig Thompson discussed the goal to move forward to take full advantage of connected and automated vehicle technology benefits, yet we need to prepare our systems where data control and data security are important for consumers and our systems. He highlighted the importance of data for all aspects of transportation and how it needs to be managed properly. There are concerns for threats today and threats tomorrow and questions about who the owners of data will be and who needs to manage this data and the connected systems. Secretary Thompson expressed his thanks for the WAVE members' diverse perspective and feedback throughout each of the previous WAVE meetings.

Meeting overview and recap of October 2022 meeting – A recap of the previous WAVE meeting highlighted updates on electric vehicles, the CAV strategic Workplan, training for law enforcement and first responders, WisDOT Bureau of Traffic Operations work, and a summary and discussion of previous WAVE member recommendations to date.

Bipartisan Infrastructure Law (BIL) Implementation – An overview of BIL related resources was provided on grant programs and the new WisDOT website. The website provides information on federal discretionary grant opportunities from U.S. DOT, dates and descriptions of grant programs, state funding programs, contacts for letters of support for local project grant applications, At-A-Glance Calendar of programs, other federal resources and tips on submitting grant applications.
WisDOT BIL Webpage – *wisconsindot.gov/BIL*

Voices of the WAVE: Committee members opportunity to highlight CAV activities in their area of work.

- **Andrea Bill, Associate Director, UW-Madison TOPS Lab –** Current work with the Racine Badger includes research on *User Trust and Pedestrian Interactions*. UW-Madison has new faculty members with expertise in CAV technologies, Xiaopeng (Shaw) and Sikai (Sky) Chen. UW has acquired two new CAV sedans and an electric CAV van to be used for new projects and is doing work with vehicle sensors, freight movements, projects to understand and explain AI algorithms, human factors, virtual reality research, infrastructure advancements and shared mobility and CAV integration.

- **Sandi Pendleton, Director, Wisconsin Technology Council –** CAV potential benefits are increasingly important in light of the data showing there are record high levels of pedestrian and bike fatalities despite unchanged miles driven. The positive news is that there are new technologies coming that can help vulnerable road users: Garmin radar/cameras for bicyclists, "Copilot" designed to provide vehicle trajectory warnings for bicyclists with cell phone connections to CVs that can warn the vehicle of bikes and pedestrians even in darkness where 77% fatalities occur.

WisDOT CAV Strategic Plan updates - link to strategic plan

- **CAV Attitudes and Perceptions Survey -** WisDOT's Policy Research program, with UW-Madison TOPS Lab, is conducting a study to survey Wisconsin's public attitudes and perceptions towards connected and automated vehicle technology. The information will inform the department on numerous factors including, but not limited to, the public's understanding of the technology, safety perspective, perceived attractiveness or rejection aspects, acceptance of testing on Wisconsin roads, factors that may encourage or discourage the purchase of CAVs, best way to converse about this topic. The cost of the study is $75,000 with the final report due December 2023.

- **Data Governance -** Data governance is a system for defining who within an organization has authority and control over data assets and how those data assets may be used. It encompasses the people, processes, and technologies required to manage and protect data assets. Benefits of data governance include the breakdown of departmental silos, creation of holistic picture of data, a single version of each database, determines security risks up front and avoids them; ensures regulatory, legal, and industry compliance; cost reduction; better, more reliable data. UW-Milwaukee's Institute for Physical Infrastructure and Transportation (IPIT) is completing the data governance research project for the agency with a final draft report due July 2023.

- **USDOT FHWA SMART grants**

  - **Autonomous Truck Mounted Attenuator (ATMA) -** The department has joined with Colorado DOT, Minnesota DOT & Oklahoma DOT, Penn State University, University of Oklahoma, and UW-Madison to test the safety and operational capabilities of an autonomous truck mounted crash attenuator (ATMA). An ATMA is designed to follow a mobile work crew with a trailer/truck that absorbs impacts from oncoming vehicles and prevents damage to both the motorist and the structure they collide with, protecting the work crew from crashes. A production ATMA vehicle removes the driver from this dangerous driving task. WisDOT's portion of the grant award is $216,000.
  - **Work Zone Data Exchange (WZDx) - Smart Work Zone Intelligent Transportation System (ITS) on Local Roads –** The department completed a test of the Work Zone Data Exchange protocol that automatically broadcasts data about work zone configurations on state highways with a 2021 FHWA grant. This new SMART grant partners with UW-Madison and the Columbia County Highway Department and expands that initial effort to include local road construction projects delivering work zone data to the Lane Closure System 2.0 automatically. These data feeds are available to transportation apps such as Wisconsin511, as well as private transportation apps and connected devices like Smart Arrow Boards.

Guest Panel: The Cybersecurity of CAVs

"What are the challenges that academia, industry, and government are facing in building resiliency?"

- Panelists outlined areas of cyber-security risks for connected vehicles and automated vehicles for members.

Guest Panel Members

- Ray Mandli, Mandli Communications
- Sia Prosper, ITS Wisconsin
- Jennifer Tisdale, GRIMM R&D
- Yiheng Feng, Purdue University

Presentation highlights

- At-Risk security entry points to vehicles or a connected intelligent transportation system can be internet connections, sensors on the vehicle, OBD- II ports, cellular radios, over-the-air update, Bluetooth, or Wi-Fi radio.
- Awareness, education and trained technical support are key resources to keep ahead of cyber-security issues.
- Security intrusions may not be noticed by humans.
- Attack surfaces and remote sensors could provide paths from infrastructure to vehicles or vehicle attacks to the infrastructure to corrupt data. Counterfeit road signs can corrupt data for vehicle decisions.
- Security Credential Management System (SCMS), Cross-validation (cross-platform) of sensor information, Security-by-design like trusted execution environment (TEE) and robust machine learning are important defenses to cyber-attacks.
- Actual successful cybersecurity vehicle intrusions are extremely rare.
- HD data mapping and other projects are continuing at the same time cyber-security threats and countermeasures are also being developed. Dynamic Mapping Centers will account for massive amounts of data, in real-time which means security in real-time is important. Car companies want data streams walled off from consumers' access for revenue purposes. It is important to keep databases segregated from outside access and only provide outside access to summary streams or dashboards. Blockchain is a valuable tool to validate over-the-air updates and other data streams.
- Everything will be connected. Car companies will push growth in entertainment and other data services they can sell.
- Most security attacks come from human weakness paths such as phishing, or weak/duplicate passwords.
- ITS Wisconsin with ITS America, FHWA and Intelligent Transportation Systems Joint Program Office (ITS JPO) offer training on cybersecurity related to transportation systems.
- Responsibilities and liabilities of interconnected systems is still evolving.

Small Group Discussions

Attendees moved into facilitated small group breakout rooms to discuss the following five questions.
A summarized list of responses to the questions can be found in **Appendix A.**

1. What stood out from the panel and the most pressing cybersecurity concern that needs to be addressed from your organization's perspective?
2. What are your organization's concerns for CAVs and cybersecurity?
3. What types of additional information does your organization need?
4. What do you feel are the State's and your organization's strengths and weaknesses when it comes to CAV cybersecurity?
5. What can be done at the State-level or at your organization to address the concerns for CAVs and cybersecurity brought up today?

Report-out of small group discussions

Each small group was asked to share main takeaway and highlights from the WAVE meeting and the small group discussions.

- Gain knowledge about threats and countermeasures.
- Collaborate with all groups.
- Education of cybersecurity in transportation is a priority.
- State should promote hands-on demos.
- Partnerships with universities are valuable.

- Recommend cybersecurity workshops and webinars with local governments and their staff to promote awareness and training.
- We must understand the whole system of data security management, where the single-entry points are and paths that provide access to the transportation system.
- Roles the different levels of government should play need to be clear and communicated.
- Partnership between private and public sector is necessary.
- Analyzing the resources available to public and private sectors needs to be reviewed.
- Be aware of the differences between urban and rural needs and resources. We need to learn what we don’t know about the needs of all groups.

Closing Remarks - WisDOT Deputy Secretary Paul Hammer thanked the members for their time and energy for today and all previous WAVE efforts to help improve WisDOT’s CAV policy, strategy, and initiatives. There are many challenges with data management and many remaining questions. It will take strong partnerships from all parties involved to work towards and realize CAV benefits. We need forums and stakeholder groups like this to bring information and ideas to the table to continue to build a safe, sustainable and equitable transportation system for everyone.

Appendix A - Sample of Responses to Small Group Questions – April 5th

Note: Only the most repeated comments are reported and summarized in this appendix.

1. What stood out from the panel and the most pressing cybersecurity concern that needs to be addressed from your organization's perspective?

Training and awareness

- Training and expertise. Not enough training in the workforce.
- Many don't believe in the level of the problem. Need to educate the public.

Technology, data and systems

- Managing large datasets security and storage.
- Data management: ownership and responsibility, public private access, MOUs, monetizing, data-based decisions.
- Awareness of multifaceted cybersecurity issues, and numerous owners of different parts of the system.
- An attack on one thing could be an entry point to attack something else. It multiplies the scope.

Legal and liability

- Liability issues (and others) are undefined. Legislation, technology, liability, private companies and public entities need to move forward together on these issues. Need a federal approach to collaborate.

Government

- Urban vs rural challenges and needs to be prepared for cybersecurity.
- What will local agencies need to do? Small municipalities have limited funding. Centralized solutions important considering funding considerations for local government transportation systems.
- Roadway Transportation Cybersecurity Work Group (federal and national organizations).

2. What are your organization's concerns for CAVs and cybersecurity?

Training and awareness

- Education of elected officials and the public.
- Enhance training in universities and tech colleges.

Technology, data and systems

- How do we know crash reconstruction data is true and accurate? Can the manufacturer be reliable in providing data accurately.
- Cybersecurity should be developed along with vehicle systems, not afterwards by government.
- Safety against vehicle hacking.

Government

- Connected systems security.- big questions – who, what, when, where & why. Unifying networks needs federal guidance.
- Legislature is not hearing much about this issue and might solve this if they are proactive. Perhaps legislators and WisDOT should discuss this. Informational hearing on possible legislation - Assembly Transportation Committee.
- Federal government is providing grants and supporting research to keep this moving.

3. What types of additional information does your organization need?

Training and awareness

- We need to train people in business and government who are coming in to do the additional work on this. We need to hire as fast as we can to develop the needed skillsets.
- Best practices in CV and AV.

Technology, data and systems

- Every group needs an asset inventory; understand institutional maturity (lots of different levels).
- Different use cases; what would different levels of government use the data for; how to make the data useful and secure; personal safety issues and other concerns.

Government

- AI will drive cybersecurity very fast. We need a committee at state level to study this.
- We need people who can figure this out and address it. We may need to get back to the Legislature to address this.
- Knowing what infrastructure is needed to make these systems run. Signage. Civil engineering requirements. Rural needs.
- Need support from federal and state government to take the lead and do more research. Information from other public entities, research entities should be shared to keep ahead on cybersecurity.

4. What do you feel are the State's and your organization's strengths and weaknesses when it comes to CAV cybersecurity?

Strengths

- This group building a professional collaboration across the state.
- That there are legislative representatives here is a strength.
- WI emergency management provides resources for emergencies. Some drills were related to cybersecurity.

Weaknesses

- Unknowns.
- Lack of urgency on the part of the Transportation Committee.
- Lack of understanding, knowledge. Convince policymakers to invest funding.
- WI emergency management. We can partner in the future to practice/tabletop related to cybersecurity.
- Opportunity to see where gaps and strengths are for the state. Understanding what we don't know.
- Municipality perspective, needing all staff members to understand the risks and the scope of vulnerability.

5. What can be done at the State-level or at your organization to address the concerns for CAVs and cybersecurity brought up today?

Training and awareness

- Awareness of cybersecurity. Talk more about what we have found and what can be corrected and the steps for the state and stakeholder.
- Need to train people to go down some of these roads. Associations within related technical fields need to bring in more members who have this headset and educate their members. Perhaps partner with tech colleges.
- Pace of change makes traditional training model outdated. We have brought in experts to talk about this in 2018. Need to focus on the AI side.

Technology, data and systems

- WAVE meetings; divvy up information needs; repositories; data storage for different organizations.

Government

- DOT has success with webinars, connecting with locals. Follow that model.
- Education road show. Drive home we are there now. Should there be demonstrations for public, vehicles and roads on Statehouse grounds.
- Some state institution should take the lead on AI – how about WisDOT?
- See the City of Madison approach, but dependent on resources. Educate staff on the security . Raise awareness and look at consequences. Work with IT professionals about exposure points and what could happen if there was a risk. Planning for recovery if an attack does happen, having a system in place if an attack does happen.