American Policymaker Safety, Privacy, and Security Preparations for Autonomous Vehicles

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Colin M. Hood
Spring, 2020

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

American Policymaker Safety, Privacy, and Security Preparations for Autonomous Vehicles

The First Autonomous Vehicle Fatality

On the night of Sunday, March 18, 2018, the headlights of a modified 2017 Volvo XC90 illuminated the roadway lighting of North Mill Avenue's two lanes in Tempe, Arizona. Outfitted with forward- and side- facing cameras, radio and light detection and ranging, navigational sensors, and a computing and data storage unit integrated into the vehicle, the XC90 was operating as one of Uber Technologies testing vehicles as part of the prototypal self-driving vehicle program (NTSB., n.d.). The vehicle operator, distracted by the center console design of the Volvo SUV, had no awareness that Elaine Herzberg, walking her bicycle across the street, had been unknowingly walking into the path of the vehicle. The SUV, charging forwards at 40mph, quickly illuminated the pedestrian in the roadway, alarming the vehicle operator just 1.3 seconds prior to its impact with the pedestrian and her bicycle This low-probability accident for the prototypal program proved to be fatal (NTSB., n.d.). While roadway accidents are unfortunately commonplace among society, ranking as the 3rd highest cause of death in the United States with six percent of the total fatalities that occurred in 2017 (Molina, 2019), the case of Elaine Herzberg was a new type of tragedy. The question of liability is immediately clouded by the lack of modern-day policy on autonomous technology; who would be deemed responsible for the first autonomous vehicle-based fatality?

Protection from Future Incidents

In order to determine who was at fault for the first fully-autonomous vehicle fatality and to prepare for the inevitability of future incidents, it is essential to know how policymakers are anticipating the emergence of new roadway technologies in common public use. The central question being explored can be explicitly defined as:

How are American Policymakers preparing for a future of autonomous vehicles with regards to protecting driver safety, privacy, and security?

In the analysis that follows, the method of documentary research analysis provides context to prior works related to autonomous vehicles. Documentary research analysis takes the findings of prior academic published works and combines both qualitative and quantitative results from various perspectives to establish a more omnipresent representation of the modern situation. To address the question regarding policy, academic works in autonomous vehicle adaptive control algorithms, safety features, and cybersecurity defenses provide an understanding of the information necessary to publish adequate policy.

The use of historical case studies, which are methods designed to analyze a situation that caused major developments in the field in the past from a retrospective viewpoint, provide quantitative evidence to some of the assertions that will be made with regards to the intent on autonomous vehicles on roadways. The development of autonomous vehicle technology combined with the tracking of general traffic statistics provides context to the motives behind pushing the release of public policy. Similarly, this use of historical case study provides a statistical metric to gauge the effectiveness of emerging policy. Public information pertaining to the hearings within the Department of Transportation congressional committees substantiates the conduct of policy analysis by looking deeper into the organization of autonomous vehicle classification and restriction. Vehicle classifications allow for the analysis of current systems and a proposal as to how different class vehicles can be accommodated in policy.

Autonomous Technology Developments

The specialty differences between the engineers designing autonomous vehicle programs and the American policymakers focused on the implementation and regulation of these vehicles

is substantial. Additionally, the limited understanding of how autonomous vehicles are equipped and operated is essential to formulating effective policy. It is in the engineers' best interests to educate policymakers in order to further continue the implementation of technological development.

Monte Carlo simulations are based on a process of using random sampling to input scenarios into a computational algorithm. Typically, the outputs of these simulations provide a more deterministic answer as to the capabilities of worst-case scenarios in an experimental run (Wang Y., et al., 2019). In the case of autonomous vehicle development, the use of the Monte Carlo method provided prototype engineers with the ability to conduct safety assessments that verified the feasibility of real-time trajectories in safety-oriented scenarios with fully autonomous response technologies (Wang Y., et al., 2019). Dr. Yijing Wang, Ph.D., and her research team have built dynamic models to ensure the safe passage of autonomous vehicles in moving traffic scenarios, and the Monte Carlo simulations they conducted allowed for the analysis of how the vehicle would respond to the dangers of automatic lane switching; these findings provide policymakers with the confirmation of the reliability of sensor perception, trajectory planning algorithms, and predictive control to optimize driver safety.

Due to the fact that Autonomous Vehicles will have to be integrated into environments with Nonautonomous Vehicles, policymakers need to ensure that the vehicles have the capability to adapt to changing obstructions along the proposed path trajectories outlined by Dr. Yijing Wang's study. The importance of the vehicle having the ability to verify long-term path trajectory and reform trajectories based on the detection and identification of potential collisions is essential due to the fact that the fully autonomous capabilities of the vehicle must encompass a feature of risk mitigation without needing driver input. Researchers have created algorithms to

receive and anticipate roadway obstructions and automatically alter course to the path of least known risk (Gruber, Althoff, 2018). This ability to interrupt a running path after the reception of new information from the vehicle's sensors is of utmost importance to creating a self-reliant vehicle that installs confidence in modern day adaptive capabilities for policymakers. Nevertheless, with multiple moving parts in the environment in which Autonomous Vehicles will be operating, there is a level of uncertainty with respect to performance that can be mitigated but not eliminated from the system. Dr. Hong Wang and her research team developed algorithms for the vehicle to identify the path of least resistance (least potential hazards) and quickly change its trajectory path to minimize damage in the case of unavoidable collision (Wang H, et al., 2019). This concept of risk mitigation and management provides policymakers with context as to the inevitability that the public will be exposed to a mitigated amount of danger with a system of Autonomous Vehicles.

An item of concern from the perspective of policymakers is the potential for cyberattack on the autonomous systems and networks being proposed by engineers. The development of robust deep learning methods to identify external exposure and secure the safety of the system has been explored by a team of engineers and implemented as a preventative security measure within Autonomous Vehicle networks (Ferdowsi et al. 2018). Cyber-physical attacks on autonomous vehicles is a concern, not only for the engineers designing the technology, but also for policymakers evaluating liability concerns and the responsibility for protecting the public from terrorist or international threats.

Departmental committee hearings conducted in 2019 identified various levels of Autonomous Vehicle technologies on today's roadways. Cars with no computer input, rear-view cameras, or steering assists are considered zero-entry vehicles, whereas fully automated vehicles

are at the top of the hierarchy (Shuster et al., 2019). Policymakers are focused on this idea of technology identification in order to develop policy that allows for an integration of technology-based vehicles into a majority nonautonomous network, and this identification method allows policymakers to elaborate on various levels of risk associated with non-autonomous infrastructure.

As seen in the case of Elaine Herzberg in Tempe, Arizona, the mixture of autonomous vehicles and pedestrians has been a concern among engineers and policymakers. The Volvo XC90 was designed to be particularly vigilant in areas designated as crosswalks; however, the capabilities of the vehicle failed in a crossing situation outside of the crosswalk. Public perception on the reliability of autonomous vehicles will determine the extent to which autonomous vehicle technology will be developed, and the findings of Brar and Caufield, who conducted a study on the impact of Autonomous Vehicles on pedestrian's safety, addressed these concerns. They found that the final measurements of "perceived safety" demonstrated that even supporters of autonomous vehicle technology do not feel comfortable with self-driving vehicles when they are in the position of the pedestrian navigating a crosswalk (Brar, Caufield, 2017). Engineers have taken the interests of both the driver and pedestrian into account, developing technology that will allow for the driver to safely and quickly navigate crosswalks as well as operate cautiously in urban environments (Schneemann, Gohl, 2016).

Certain cities are available to policymakers to be used as examples for further analysis. Legal "guardrails" have allowed cities like San Francisco and Oakland to use data sharing amongst autonomous vehicles in order to improve roadway connectedness (Rodriguez, 2019). Privacy implications and liability issues of autonomous vehicles, attempts to address how certain social demographics will be harmed or potentially backlash against systems that expose user data

to a larger public (Collingwood, 2017), making the public one of the most influential stakeholders in the implementation of autonomous vehicle technology. Engineers are accounting for concerns in privacy protection, creating systems with privacy-preserving efforts as the main objective (Hadian, Altuwaiyan, Liang, Zhu, 2019). These assertions provide policymakers with further concerns to ensure the equal and effective regulations being placed on Autonomous Vehicle operation—based on the results of prior implementation.

Studies conducted to predict the impact of Autonomous Vehicles and the ability to connect with one another have identified a potential to reduce the total amount of collisions on roadways. A particular study discusses predictive statistics behind how much safer autonomous vehicles would be on roadways without manually operated cars. The findings provide very significant percentages with regards to collisions that could have been prevented—some being as high as 90-94% deterrence (Papadoulis, Quddus, Imprialou, 2019). Another safety strategy as discussed within, Assuring Fully Autonomous Vehicles Safety by Design: The Autonomous Vehicle Control (AVC) Module Strategy, defined a way to develop a protection layer around the autonomous vehicle that is independent of the way the vehicles system was developed—similar to the techniques of machine learning (Molina et al., 2017). This information could provide an argument that autonomous vehicle technology may develop on its own, with fewer and fewer needs for human input. As the technology continues to develop, algorithms that can detect and process outside information may be able to do so faster than human-created algorithms.

The studies conducted within Privacy-Preserving Task Scheduling for Time-Sharing Services of Autonomous Vehicles, demonstrate that efforts are being made to create a system with privacy-preserving efforts as the main goal (Hadian, Altuwaiyan, Liang, Zhu, 2019). This addresses a potential for privacy-breaching systems that would put users at higher risk. The

legality of sharing user data among autonomous vehicle networks and party-sharing systems is outlined in privacy implications and liability issues of autonomous vehicles, and describes how certain social demographics will be harmed or potentially backlash against systems that expose user data to large pools of users (Collingwood, 2017). The downside of party-sharing systems is that users no longer have the ability to move about in relative anonymity—making privacy nonexistent.

Social Construction of Technology, Risk Analysis, and Autonomous Vehicles

The STS framework of the societal construction of technology (SCOT) and how it is incorporated in the development of American Policy with regards to Autonomous Vehicle technology on roadways is the overarching topic to address throughout the documentary research analysis. The societal construction of technology perspective is focused on how the public responds to emerging technologies, and supports the claim that the response to technology further drives its development (Klein, Kleinman 2002). In the case of Autonomous Vehicle technology, this idea that popular opinion is the driving factor in the shape of modern technology is supported by the increasing interest to automate roadways based on the media's analysis of its impact on decreasing traffic dangers and fatality statistics. Policymakers take a SCOT perspective on developing Autonomous Vehicle policy when faced with major corporations implementing prototype programs through preexisting legal loopholes, as seen in San Francisco and Oakland. This pressure to expedite the policymaking process is driven from consumer interest motivating large corporations to put in place autonomous programs to improve efficient operation.

A further breakdown of how each stakeholder in the problem (policymakers, engineers, and the public) will add to the SCOT framework will be included to organize sources and build a

universal understanding of the situation. The timeline of the paper involved conducting further research pertaining to how far the implementation of autonomous vehicles has gone in society thus far. After an understanding of current policy had been formed, avenues suggesting the longevity of autonomous vehicles and policy creation was sought out. The assembly of information is designed to provide an understanding of the perspective of policy makers and further criticize the current system and its flaws.

American Policymakers are also faced with interpreting research and technological developments from a risk analysis perspective, as defined by theorist Ulrich Beck. Beck identifies risk mitigation in society as, "a systematic way of dealing with hazards and insecurities induced and introduced by modernization itself," similar to the techniques developed by Dr. Hong Wang and her research team that worked to address hazards caused by modern technology problems and set the vehicle on the path of least damage (Beck, 1992). By viewing autonomous technologies from the risk analysis perspective, policymakers ensure that they identified every possible worst-case scenario. Taking this perspective, tragedies like the occurrence of the Elaine Herzberg incident would be assigned a risk probability and assessed as to the risk each incident poses to the ethical implementation of Autonomous Vehicles on roadways.

Current Policy Protection and Implementation

The Subcommittee on Highways and Transit is focused on three main aspects of regulating the implementation of autonomous vehicles into the surface transportation system. These include: the physical threat that autonomous vehicles pose to non-autonomous vehicles, the cyber-physical threat that unsecure systems pose to the safety and privacy of occupants in autonomous vehicles, and the viability to enforce regulations on autonomous vehicles in the current roadway system. The mission of the National Highway Traffic Safety Administration is

to “save lives, prevent injuries, and reduce economic costs due to road traffic crashes, through education, research, safety standards, and enforcement activity” (“Automated Driving Systems”, 2017). To enforce this mission, particularly on autonomous vehicles, the Department of Transportation asks States to maintain the delineation of Federal and State regulatory authority. This maintains the balance between States looking for Federal entities to ensure safe roadways while allowing states to enact more strict legislation, but what federal mandates ensure a baseline standard for use of autonomous vehicles on roadways?

The most relevant safety standard pertaining to the control of automotive electronic systems is mandated under ISO 26262, a risk-based safety standard for functional safety (Van Eikema Hommes, 2016). ISO 26262, or “Road vehicles—functional safety”, regulates driver assistance, propulsion, and vehicle dynamics control systems with regards to the electronic systems powering them. The regulation requires producers to compile a qualification plan, documentation, classification analysis, and a qualification report for the software tools the producer implements in the vehicles design (Bellairs, n.d.). The legal implications of ISO 26262 ensure the safe production of autonomous vehicles to validate that producers are putting their vehicles through the necessary tests, like those of Dr. Yijing Wang’s research team and their dynamic models and Monte Carlo simulations to test compliant autonomous systems (Wang, Y. et al., 2019).

When examining the Federal Motor Vehicle Safety Standards (FMVSS), the regulations established for vehicle design, construction, and performance, the National Highway Traffic Safety Administration has identified potential barriers and challenges for the certification process of automated vehicles (Kim, et al., 2016). The analysis performed by the National Highway Traffic Safety Administration separated classification of autonomy from limited to highly

automated, driverless concepts following the same qualities mentioned in the hierarchy established in the Shuster's departmental committee hearings (Shuster et al., 2019). The main challenge is that FMVSS does not explicitly address automated vehicle technology and often assumes the presence of a human driver (Kim, et al., 2016). The conclusion of the analysis found that if autonomous vehicles remain in the boundaries of conventional design (cabin layouts, light configurations) the issues this driverless challenge presents only rest in theft protection and rollaway prevention (§571.114) and light vehicle brake systems (§ 571.135). Adding to this analysis from the angle of a historical case study, the situation in Tempe Arizona and the failure of a light vehicle's braking system resulted in the first autonomous vehicle caused fatality in the United States (NTSB, n.d.)—demonstrating the necessity of an expedited FMVSS policy change.

Automotive Open System Architecture, AUTOSAR, presents cyber security concerns among the automotive industry with regards to system operation and privacy safety. The goal of the AUTOSAR organization and safety standards are defined by need needs: to fulfill future vehicle requirements, such as availability and safety, to accelerate development and maintenance, to improve containment of product and process complexity and risk, and to optimize costs of scalable autonomous vehicle systems (Yu, Lin, 2016). The ability for vehicles to identify and conceptualize the idea of pursuing the least-risk trajectories, as analyzed in the experiments of German mechatronic engineers Felix Gruber and Matthias Althoff (Gruber, Althoff, 2018), has been pursued by the AUTOSAR program, and is a necessity of new driverless vehicles being produced. Similarly, the algorithms of Dr. Hong Wang's research team set the standard for acceptable risk mitigation set forth by the AUTOSAR program (Wang, G, et al., 2019). The two regulatory policies, AUTOSAR and ISO 26262, were developed around the same time, and the AUTOSAR program references ISO 26262 for safety considerations.

The Motor Industry Software Reliability Association (MISRA) set forth the guidelines to facilitate code safety, security, portability, and reliability in embedded systems ("Protecting Embedded Systems with New MISRA C Guidelines", 2017). The association is a collaboration between manufacturers, component suppliers, and engineering consultancies to promote the highest standards of safety and security related electronic systems and software-intensive applications. While MISRA C is a voluntary automotive industry standard for the use of C language in safety-related automotive embedded systems, it is widely accepted among car manufacturers as the standard for implementing software-controlled electronic systems (Burden, Tapp, 2016). ISO 26262 recommends following MISRA C for software coding, and it is a supporting standard that outlines instances of the C language to emphasize safety concerns—focusing on programmer errors, compiler variations and errors, and potential poor performance in run-time checking.

While AUTOSAR focuses on system architecture design and MISRA C focuses on software coding rules, both agencies are recommendations for manufacturer compliance, and cyber-physical attacks on autonomous vehicles is still a large concern for effective implementation of the technology onto roadways. The ultimate solution to identifying an external attack on the autonomous vehicle's system rests in developing robust learning methods to promote preventative invasive measures on vehicle systems, similar to the proposals of Aidin Ferdowsi, PhD Candidate at Virginia Tech (Ferdowsi et al. 2018). The research team directed by Dr. Hadian, putting together privacy-preserving efforts into the software, can also be implemented by car manufacturers to prevent the utility of a hack by malicious intent (Hadian, Altuwaiyan, Liang, Zhu, 2019). This idea that a self-contained system with the ability to identify outside influence and disable the threat of an offensive hack would provide car manufacturers

with a tool to implement in compliance with the one of the five goals of the cybersecurity research program: “strengthen and facilitate the implementation of safety-effective voluntary industry-based standards for automotive electronics reliability” (Van Eikema Hommes, 2016). Risk analysis, as emphasized by Ulrich Beck’s ideas within World Risk Society, suggests that this accommodation of a hack-threat or privacy-breach will promote public favor of the cost/benefit argument as to whether autonomous vehicles will be deemed to be a viable pursuit to society’s interest (Beck, 1992). If the risks involved with autonomous vehicles and consumer privacy is too high, the concerns of society will phase out the technology on roadways by shifting the public’s interests to less risky avenues of transportation.

In the Department of Transportation’s Preparing for the Future of Transportation, in 2018, the federal government affirmed the approach for car manufacturers to make their voluntary safety self-assessments public to provide transparency and confidence in the technology in order to provide the American people with more information about potential risks (“Autonomous Vehicles 3.0”, 2018). This strategy of allowing manufacturers to embrace voluntary standards, newly emerging research, and pursuing the best practices for their stakeholders allows the innovation of the technology to progress without impact of the slow pace of bureaucracy. The report states that the Department of Transportation intends to stay removed from the regulatory process in order to promote a healthy balance between safety and innovation. The US DOT suggests that there is a federal role in automation research, largely in the advocacy for stem-based programs to conduct independent studies and publicly release their findings, but this lack of regulation leaves the necessity of regulation up to the determination of the states. While this differs from the federal influence on the transportation industries of train or airplane-

based travel, it prompts manufacturers to enhance their technologies in order to satisfy their own economic interests—like sales and stakeholders.

In this federally mandated but state-restricted situation with regards to the regulations on autonomous vehicles, certain states are less deterring than others when it comes to the enforcement and implementation of autonomous technologies on roadways. For instance, the general consensus in the state of Louisiana is to place as little restriction and regulation on the development of autonomous vehicles as possible so that innovation is inhibited as little as possible (Wilmot, Greensword, 2016). The uniformity of a federal standardization is welcomed by the state of Louisiana but the current situation consists mainly of federal suggestions to car manufacturers and not state law enforcements. The proposals of the federal government suggest the philosophy of removing the threat before it enters the system so that state governments do not have an invasive risk to then develop separate legislation and exercise new methods of law enforcement and detection. The studies of attorney Gregory Rodriguez found that these federal suggestions and state freedoms lead to the creation of legal ambiguities where vehicles do not have to restrict or close data sharing among other autonomous systems on the roadway, leaving potential privacy security threats at large (Rodriguez, 2019). This evidence of state's rights with regards to roadway limitations accentuates the ideology of the social construction of technology with regards to the development of policy (Klein, Kleinman 2002). The freedoms established by the federal government allow for the development of state policy, reflecting the interests of multiple different groups of society to piece together unique legislation with the balance between supporting innovation and protecting public safety.

The focus of the study of autonomous vehicle legislation was limited to federal policy and explored examples of state-based policies and implementation. To broaden the scope of the

project, an analysis of each state's autonomous vehicle policy provides a clearer image to how unique state policy has become based on independent development. Further limited, this study does not look at the differences in standards specific auto manufacturers put into the development of autonomous vehicle software. While it was explored that the federal government may make recommendations to auto manufacturers, discovering what software-based differences and how they were shaped provides a more detailed account of the modern situation. Limitations were taken in an effort to consolidate the main policies influencing autonomous vehicle development and make a more precise recommendation.

To further expand on developing higher federal standards for autonomous vehicle technology, a study can be made to examine how strictly regulated car manufacturers are with regard to how they develop autonomous software. Tackling this perspective of vehicle development instead of roadway regulation will prevent automakers from releasing potentially dangerous vehicles onto streets in the first place. A recommendation targeted at car manufacturers would be an excellent continuation of the study in order to closely monitor software-based development.

Balancing Innovation Speed and Safety

The two avenues of American policy, federal and state, take separate approaches to accommodate the ideas of protecting the physical safety of autonomous and nonautonomous vehicles, enhancing the cybersecurity standards for software-oriented electronic systems, and putting together enforceable legislation for proper regulation. While the federal government has policies like ISO 26262, requiring manufacturers to report all the software-driven aspects of a vehicle's capabilities, the federal government fails to adapt other legislation like FMVSS to the developing automotive technologies of today's society which presents further risks. One of the

most important roles of the federal government rests in making recommendations to car manufacturers and state legislations, like recommending adherence and enforcement of the standards outlined by the AUTOSAR and MISRA organizations. Leaving regulations relaxed, the federal government has promoted state legislations to adopt unique regulations on autonomous technology, which has allowed for a more appropriate account of constituent concerns and interests—allowing the American people to shape American Policy on autonomous technology.

References

Automated Driving Systems: A Vision for Safety (p. 36). (2017). Department of Transportation. https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

Automated Vehicles 3.0: Preparing for the Future of Transportation. (2018). https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf

Beck, U., & Ritter, M. (1992). Risk society: Towards a new modernity. London: Sage Publications.

Bellairs, R. (n.d.). What Is ISO 26262? An Overview. Perforce Software. Retrieved February 21, 2020, from https://www.perforce.com/blog/qac/what-iso-26262-overview

Brar, J. S., & Caulfield, B. (2017). Impact of autonomous vehicles on pedestrians' safety. 2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC), 714–719. https://doi.org/10.1109/ITSC.2017.8317963

Burden, P., & Tapp, C. (2016). MISRA Compliance: 2016. Achieving Compliance with MISRA Coding Guidelines. https://www.misra.org.uk/LinkClick.aspx?fileticket=w_Syhpkf7xA%3D&tabid=57

Collingwood, L. (2017). Privacy implications and liability issues of autonomous vehicles. Information & Communications Technology Law, 26(1), 32–45. https://doi.org/10.1080/13600834.2017.1269871

Ferdowsi, A., Challita, U., Saad, W., & Mandayam, N. B. (2018). Robust Deep Reinforcement Learning for Security and Safety in Autonomous Vehicle Systems. 2018 21st

International Conference on Intelligent Transportation Systems (ITSC), 307–312. https://doi.org/10.1109/ITSC.2018.8569635

Gruber, F., & Althoff, M. (2018). Anytime Safety Verification of Autonomous Vehicles. 2018 21st International Conference on Intelligent Transportation Systems (ITSC), 1708–1714. https://doi.org/10.1109/ITSC.2018.8569950

Hadian, M., Altuwaiyan, T., Liang, X., & Zhu, H. (2019). Privacy-Preserving Task Scheduling for Time-Sharing Services of Autonomous Vehicles. IEEE Transactions on Vehicular Technology, 68(6), 5260–5270. https://doi.org/10.1109/TVT.2019.2909468

Heron, M. (2019). Deaths: Leading Causes for 2017. 77. (Report No. DOT HS 812 069). Washington, DC: National Highway Traffic Safety Administration.

Kim, Anita, L., Perlman, D., Bogard, D., & Harringotn, R. (2016). Review of Federal Motor Vehicle Safety Standards (FMVSS) for Automated Vehicles. 148.

Klein, H. K., & Kleinman, D. L. (2002). The Social Construction of Technology: Structural Considerations. Science, Technology, & Human Values, 27(1), 28–52. https://doi.org/10.1177/016224390202700102

NTSB. (n.d.). PRELIMINARY REPORT HIGHWAY HWY18MH010. Retrieved January 31, 2020, from https://www.ntsb.gov/investigations/AccidentReports/Reports /HWY18MH010-prelim.pdf

Protecting Embedded Systems with New MISRA C Guidelines. (2017, May 2). LDRA. https://ldra.com/protecting-embedded-systems-new-misra-c-guidelines/

Rodriguez, G. (2019). Autonomous Vehicles and Unmanned Aerial Systems: Data Collection and Liability [Leading Edge]. IEEE Technology and Society Magazine, 38(3), 14–16. https://doi.org/10.1109/MTS.2019.2930264

Schneemann, F., & Gohl, I. (2016). Analyzing driver-pedestrian interaction at crosswalks: A contribution to autonomous driving in urban environments. 2016 IEEE Intelligent Vehicles Symposium (IV), 38–43. https://doi.org/10.1109/IVS.2016.7535361

Shuster, B., Young, D., Petri, T. E., Coble, H., Carolina, N., Duncan, J. J., … Hunter, D. (n.d.). COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE. New York, 89.

Van Eikema Hommes, Q. D. (2016, June). Assessment of safety standards for automotive electronic control systems. (Report No. DOT HS 812 285). Washington, DC: National Highway Traffic Safety Administration.

Wang, H., Huang, Y., Khajepour, A., Zhang, Y., Rasekhipour, Y., & Cao, D. (2019). Crash Mitigation in Motion Planning for Autonomous Vehicles. IEEE Transactions on Intelligent Transportation Systems, 20(9), 3313–3323. https://doi.org/10.1109/TITS.2018.2873921

Wang, Y., Liu, Z., Zuo, Z., Li, Z., Wang, L., & Luo, X. (2019). Trajectory Planning and Safety Assessment of Autonomous Vehicles Based on Motion Prediction and Model Predictive Control. IEEE Transactions on Vehicular Technology, 68(9), 8546–8556. https://doi.org/10.1109/TVT.2019.2930684

Wilmot, C., & Greensword, M. (2016). Investigation into Legislative Action Needed to Accommodate the Future Safe Operation of Autonomous Vehicles in the State of Louisiana [Louisiana Transportation Research Center].

Yu, H., & Lin, C.-W. (2016). Security concerns for automotive communication and software architecture. 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 600–603. https://doi.org/10.1109/INFCOMW.2016.7562147