



Docket #NHTSA 2018-0092

December 10, 2018

National Highway Traffic Safety Administration
U.S. Department of Transportation (DOT)
1200 New Jersey Avenue S.E.
Washington, DC 20590

In RE Advance Notice of Proposed Rulemaking: *Pilot Program for Collaborative Research on Motor Vehicles with High or Full Driving Automation*

On behalf of Rajant Corporation, thank you for the opportunity to address the salient issues regarding Automated Vehicle (AV) testing and research.

About Rajant Corporation:

Rajant Corporation develops, manufactures and deploys highly secure wireless communications technology. Rajant was the first to build for the U. S. Military its patented Kinetic Mesh® technologies using Rajant's BreadCrumb® wireless LAN technology. These network components are designed for rugged terrains and harsh physical environments like those seen by troops in the field. Our technologies are battle-proven to support the mission-critical communications they need to simultaneously overcome the challenges of environmental adversity and security. Rajant's key differentiation point, its ability to maintain connectivity while assets are mobile, is the cornerstone of Rajant's success. Rajant has a proven track record of performance in a number of high-profile military programs, such as C-Ram. Certain of our military products have achieved NSA certification which mandate the highest level of security requirements be met prior to being fielded within the Department of Defense (DOD), and thus, are designed to ensure secure transmission and reception of highly sensitive information in combat conditions – conditions where a breach in confidentiality could result in fatal consequences.

Rajant is an industry expert in secure wireless and mobile wireless communications, data encryption and protection, data authentication, cybersecurity and integrity. Our comments below focus on our area of scientific, implementation and policy expertise: cyber security and data integrity.

NHTSA Should Conduct Its Own Pilot Testing Program

Rajant agrees with other commenters that NHTSA and US DOT should proceed with its own pilot testing program and/or programs. Such testing would not preclude ongoing industry, academic and NGO research, but would allow for impartiality that is highly difficult to achieve in both the private and not-for-profit arenas. NHTSA and US DOT have a long and distinguished record of high-level research, testing and leading the implementation of highway and vehicle safety innovations as well as the unique ability to collect and synthesize information from the many AV interests. NHTSA and US DOT technical advisory committees can provide critical expertise to such an effort.

It is the opinion of Rajant that NHTSA and US DOT is well-placed to promulgate independent, impartial and robust research testing and should proceed with pilot testing and research.

NHTSA Authority Regarding Cyber Security and Integrity

200 Chesterfield Parkway • Malvern, PA 19355 • tel (484) 595-0233 • fax (484) 595-0244

www.rajant.com



NHTSA has not addressed operational cyber risk in vehicles currently approved for sale and use by the public. This lack of regulation may be justified for the current vehicle fleet in that automotive systems connected via wireless are limited to navigation, communications and other information systems which are largely unrelated to safety and performance.

AVs, however, will likely operate with integrated systems which are connected via wireless communication protocols. Such systems may include features such as over-the-air software updates, Vehicle to Vehicle (V2V) communications and Vehicle to Infrastructure (V2I) systems. The integration of such systems and the resultant wireless connection(s) therefore make cyber risk a significant safety issue and thus a direct, and primary responsibility of NHTSA.

In the interest of automotive and public safety, Rajant believes NHTSA should take the lead and coordinating role in requiring robust cyber security measures. An NHTSA-managed pilot program is the ideal opportunity to test and implement robust cyber security measures.

Rajant recommends NHTSA lead, coordinate and implement robust cyber security requirements and include cyber security and reducing cyber risk as a prime goal in any pilot program.

Critical Importance of NHTSA Standards in Cyber Integrity and Data Protection

Unlike previous advancements in vehicle electronics, the safety and performance systems in AVs are integrated throughout the vehicle and are proposed to have wireless connections for over-the-air updates, to remote control centers, infrastructure (V2I) and other AVs (V2V). Thus, currently what amounts to a firewall between systems connected via wireless (information, cell phone, and entertainment systems) and safety and performance controls will not exist in Levels 4 and 5. Such interconnectedness will put critical safety and performance systems at risk for cyber-attack, vulnerabilities in original coding and/or over-the-air updates. Further, maintaining the integrity and robustness of this new network and the data that travels through it must be a primary consideration. NHTSA therefore should be considered the primary regulatory body for AV cyber integrity.

The Rajant comment to AV 3.0 highlighted important sections regarding cybersecurity of the report the Rand Corporation has submitted as comment to the NHTSA Pilot Program ANPRM (*Measuring Automated Vehicle Safety: Forging a Framework* (2018)). We at Rajant are including those sections in this comment and endorse the below text. We believe the Rand Corporation's insights are critical and should be given a high priority consideration.

AVs are particularly vulnerable to cybersecurity attacks because they are made of computer-based systems—in technical jargon, AVs are cyber-physical systems or systems that embed computer-based elements in something that operates or interacts in the physical world. The transition toward AVs will only increase reliance on inevitably vulnerable hardware and software, both susceptible to cybersecurity problems. Recent experience by banks, utilities, and even the federal government suggest that successful cyberattacks are likely. The automotive industry's relative inexperience in addressing this risk also suggests caution should be exercised. (RAND: p. 52)

Cybersecurity for AVs will be further complicated as communications from the outside grow. Many concepts of AV operation rely at least in part on some kind of connectivity with other vehicles, infrastructure, or the internet. This connectivity is probably necessary, but it also increases cybersecurity risks. Even for conventional

vehicles, over-the-air communication could (and to some extent already does) take place for diagnostic or updating purposes. (RAND: p. 53)

The risks of a cybersecurity failure are considerable. At the lowest level, unsophisticated actors could cause simple vandalism by preventing the operation of parts of the vehicle, with safety consequences at varying levels of severity (e.g., preventing the opening of windows, interfering with the operation of brakes). Ransomware attacks, in which a perpetrator demands compensation (increasingly using anonymous cryptocurrencies) in return for restoring control of a software system, could be a viable business model for some criminal groups, which might be in other countries outside the easy reach of U.S. law enforcement. Relatively detailed personal data (including audio, video, and location data) could be collected and exploited. Large-scale terrorist or foreign nation-state attacks exploiting the same software or hardware vulnerabilities and utilizing numerous vehicles to attack critical infrastructure could cause mass casualties or sow panic. (RAND: p. 53)

While cybersecurity is of critical concern, it is distinct enough from other safety risks that it deserves separate treatment elsewhere. ... A hacker will probably not reveal that she has found a critical vulnerability until after that vulnerability is exploited and the damage is done. (RAND: p. 53)

Given the national security risks involved, the probable inability of the civil justice system to create adequate incentives for the scale of risks, and the historic role of other nation-states in cyberattacks, there is a strong argument for the involvement of the federal government in both leading and requiring strong cybersecurity protections. (RAND: pp. 53-43)

Lack of Cyber Integrity Requirements Reduces Potential Safety Benefits

Removing human error in the operation of motor vehicles may result in significant public benefits, including reduced deaths, injuries and property damage. It is a mistake, however, to assume that deployment of AV will automatically facilitate such benefits. Deployment of AV without robust cyber security and cyber integrity protections has the potential to undermine and/or significantly delay such potential benefits.

Cyber risk is a function of both the sophistication of the intruder and the number of threat vectors (i.e. an avenue through which the intruder has access). The world and its economies have seen intruders become more sophisticated and aggressive in their techniques and abilities. Both state and non-state actors possess the ability to disrupt, infect, exploit and disable systems throughout the world. Limiting the technical advances by intruders is impossible; but staying one step ahead and enhancing security and redundancy is a never-rest proposition. Similarly, the number of threat vectors will continue to increase as the Internet of Things becomes ever present and prolific (and AVs are part of the emergent Internet of Things). Every electronic system connected via wireless communication is a potential threat vector.



The path forward for defense against exploitation is sophisticated cyber security software and hardware designs which block intruders at each and every potential threat vector. Typically, intruders will mount multiple attacks with multiple objectives, seeking vulnerabilities in a system, be it through hardware, software or firmware. Entry is gained via the least secure (or unsecured) threat vector. For AV, two likely future scenarios present significant cyber risk: 1) Over-the-air software updates; and 2) V2V and V2I communication data paths. In both instances critical safety and performance systems will be accessed via wireless communication, creating new threat vectors through which intruders can access critical systems.

Cyber Risk Danger for AVs and Reduction of Benefits

Cost-benefit analyses that assumes away human error while assigning zero or near zero error from ADSs is fundamentally flawed. In addition to the empirical evidence of the problems that the current technology has, this methodology fails to consider the historic means to exploit historically used by those of bad intent. Unless appropriate protections are embedded in AVs and AV infrastructure, intruders will have the opportunity to successfully attack the ADS. While outright “hijacking” of an AV may become less likely, it cannot be ignored that multiple and coordinated attempts will be made to infiltrate AV’s. More likely, there is a dangerous potential that intruders will have the ability to engage in data theft, insertion of malware, data destruction and control or disablement of vital systems. An ADS that automatically shuts down if it detects unusual behavior (which also would be a software program at risk of being hacked) remains a problem as the hacker does not need to take control of the vehicle, but just has to trigger the detection of unusual behavior to cause a disablement.

The danger for the AV industry is very high. Aside from the possibility of disablement causing crashes, injuries and property damage, the AV industry would necessarily experience a loss in public confidence. In comparison, consider airline industry safety. An accident rate of 1 fatal incident per 100,000 flights in the United States would mean at least one fatal incident per week – and we suggest that the public would regard that as intolerable. Any failure to address cyber risk from the increasing sophistication of intruders and increasing number of threat vectors could result in frequent disablement incidents and a loss of public confidence in AVs. Such a loss of confidence would harm the industry, resulting in delays in the reduction of deaths, injuries and property damage from human error (in effect, *causing* death, injury and property damage).

An NHTSA pilot program would greatly benefit the public and the AV industry as such a program provides the opportunity to conduct a transparent, comprehensive cost-benefit analysis of the technology and all risks associated with AV technology. A pilot program is the perfect venue to test robust cybersecurity protocols and incorporate the benefits of rigorous protections into the cost-benefit analysis.

Rajant recognizes the Agency’s preference that each question within the ANPRM be answered sequentially. However, the specific cybersecurity recommendations discussed below apply to multiple questions. The comment is organized with a detailed discussion of each cybersecurity issue (Data Authentication, Data-At-Rest Protections and Secure Software) and a specification of which question in the ANRPM is applicable. Each cybersecurity issue is applicable to Question #1.

Data Authentication [Question #1; Question #11 (a), (A) (B, v); Question #13(a), (b), (c), (k)]



Rajant has expertise in vital areas of cybersecurity and integrity: Data authentication and protection of data-at-rest. NHTSA can significantly reduce cyber risk for AVs and AV infrastructure by adopting robust requirements in both areas. Furthermore, the cybersecurity industry has the ability to implement systems and procedures today to reduce cyber risk tomorrow.

Defining Data Authentication

Data authentication is the process by which a digital system confirms that the data it receives is true and not false or corrupted. In order to operate any ADS must process multiple streams of data from the AV sensors. Such information is used to make operating decisions such as proximity detection, condition and systems monitoring braking, acceleration, and steering. Critically, the ADS must receive information that is accurate and authentic upon which to base its decisions. If a hacker is able to communicate to the ADS and transmit false data, the ADS will not be able to function in a safe manner. It is thus necessary for the ADS to authenticate the data it receives virtually instantaneously.

Data authentication becomes more vital as the number of threat vectors increases. Not only is each sensor a threat vector, but V2V and V2I communication is an additional threat vector. Furthermore, each communication from the sensors, V2V and V2I requires data authentication in order to confirm that the information is correct and allow the ADS to operate safely and efficiently.

Rajant Recommends that robust data authentication be embedded into every ADS, starting with the pilot testing program.

Question #11 (a): Data authentication is a necessary component of Safety Element #7 in "A Vision for Safety."

Question #11: (A) Data authentication is vital to reduce the risk of failure; (B, v) ensure the safety of software updates; (B, viii) and in post-deployment ADS updating.

Question #12: Data authentication is a vital area of safety and security not directly addressed thus far in NHTSA or US DOT guidance.

Question #13: (a) Data authentication should be required of participants in any NHTSA or US DOT pilot program in determining the safety capabilities of the ADS; (k) the safety of software updates; (n) and post-deployment ADS updating (n).

Data-At-Rest [Question #1; Question #10(b), (c), (d); Question #11(a), (A), (B, v); Question #12; Question #13(a), (e), (f), (k), (n); Question #15]

Data-At-Rest is simply any data not currently in active use. The high-profile breaches of business, where financial and personal data are stolen are breaches in the protection of data-at-rest. In the case of AVs, such data would include information on the performance of the vehicle, where the vehicle has traveled, how the ADS is operating, etc. Theft of data-at-rest may not pose an immediate risk to the performance and safe operation of an AV, but it does pose significant other risks, including violation of privacy and hindrance of the ability to investigate accidents. Accurate data has the ability to



provide additional important benefits, such as facilitation of future innovation, improvements in public infrastructure and calculation of insurance premiums. Rajant believes that protection for data-at-rest is not only a requirement for safety but would also deliver very high benefits as compared to the cost.

Protections for data-at-rest are important to facilitate not only NHTSA investigation of any crash or other salient incident, but also for future determination of causation and liability of crashes or litigated incidents upon public deployment of Level 4 and 5 vehicles. Although US DOT has stated that liability is a responsibility of the states and, where applicable, other non-federal jurisdictions, a federal standard for the protection of data related to product liability would satisfy US DOT policy to avert a patchwork of confusing and potentially conflicting regulations. In addition, setting such standard would not be a federal determination of who is legally responsible for any incident as that would, as DOT has indicated already, be left to other jurisdictions to determine.

Currently and in most vehicles, critical safety systems and data are physically separated from wireless connections. Thus, protection of data at rest is of a lower priority. As stated above, the status quo is highly likely to change. AV companies have considered a wide variety of uses, including remote, wireless control of vehicles and fleets as well as over-the-air updates that extend well beyond information systems and into critical vehicle safety and control systems. In such a state of existence, data at rest is accessible via remote connection and the potential to alter, steal or corrupt such data becomes a risk.

Rajant defers to the appropriate parties to recommend what data is necessary to retain and in what form.

Question #10: (b) Data-at-rest protection is necessary to maintain privacy, (c) allow for secure data storage, (d) and allow for accurate retention and reporting.

Question #11: (B, v) Data-at-rest protection is necessary to ensure the safety and security of software updates.

Question #12: Data-at-rest protection is a vital area of safety and security not directly addressed thus far in NHTSA or US DOT guidance.

Question #13: (a) Data-at-rest protections should be required of participants in any NHTSA or US DOT pilot program in determining the safety capabilities of the ADS; (e) security of reporting data; (f) in order to facilitate any possible investigation or enforcement action by NHTSA; (k) security of software updates; (n) and post-deployment maintenance.

Question #15: Data-at-rest protections should be required to help ensure that any data requested by NHTSA is not corrupted.

Secure Software Boot

To be secure, embedded systems need to have secure booting capabilities. Secure booting is a component of a processors' operating system aimed at preventing malicious software applications and "unauthorized" operating systems from loading during the system start-up process. In short it means the ability of the computer systems in an AV or part of AV infrastructure in to start (i.e., boot) securely such that the



Software Boot allows only trusted and verified downloads to the system and/or trusted and verified reprogramming of the system. This is critical to the safe operation of AVs.

Related to both Data-At-Rest and Data Authentication, protections need to be in place to ensure that the Software Boot images executed by the ADS are authenticated prior to loading and executing. **In order to ensure proper cyber security, a hardware-based Secure Software Boot mechanism should be used.**

Rajant recommends that a hardware-based Secure Boot mechanism be implemented in all AVs in order to ensure safe operation and prevent the introduction of viruses and/or malware into the ADS.

Question #11: (a) Hardware-based Secure Boot mechanism is a necessary component of Safety Element #7 in "A Vision for Safety."

Question #11: (B, v) Secure Software Boot is necessary to allow for the safety of software updates and (B, viii) post-deployment ADS updating and maintenance.

Question #12: Secure Software Boot is a vital area of safety and security not directly addressed thus far in NHTSA or US DOT guidance.

Question #13: (a) Secure Software Boot should be required of participants in any NHTSA or US DOT pilot program in determining the safety capabilities of the ADS; (k) security of software updates; (n) and post-deployment maintenance.

Exemptions (Question #14; Question #16)

Rajant recognizes the importance of exemptions in order to advance testing. However, we do not believe that exemptions should be granted for data authentication or data-at-rest protections. Both data authentication and data-at-rest protection are necessary design elements for public deployment of Level 4 and 5 vehicles and thus should be a prerequisite for any pilot testing program. As enumerated above, such protections must be part of the embedded design of any AV for the purposes of public safety and public confidence in AVs. In the world of AV deployment, exempting data authentication or data-at-rest protections is akin to exempting the inclusion of brakes in conventional vehicles.

Rajant recommends that data authentication protocols and data-at-rest protections be required of all vehicles in any testing program and all AVs deployed on public thoroughfares without exemption.

Data Authentication, Data-At-Rest Requirements, and Secure Software Boot Are Not Likely to Delay Public AV Deployment

NHTSA is rightly concerned that unnecessary delays in the adoption of AVs may delay the potentially significant benefits of reducing the number of deaths, injuries and property damage due to human error. However, the inclusion of robust data authentication and data-at-rest protection requirements by NHTSA will not contribute to that delay, in the opinion of Rajant.

It is well documented that AVs still have great difficulty in many common situations which historically have been navigated by human drivers. Among the difficult challenges AVs face are: operating in conditions of adverse weather and recognizing common cues from human drivers and pedestrians, such as waving a car forward or operator fatigue. In addition, industry has yet to determine issues such as exterior signaling devices, extent and type of V2I and V2V communication, and types of



sensors to use, among other challenges. Solving these very difficult problems and determining the most efficient and effective standards will be necessary before AVs can be deployed in large numbers.

It is the expert opinion of Rajant that addressing the problem of data authentication and implementing data-at-rest protections can be done in parallel to the many challenges facing AV deployment and accomplished in a timely manner and are necessary for the safe development and use of autonomous vehicles. As such, data authentication and data-at-rest requirements promulgated by NHTSA will not result in delay of AV deployment and thus will not negatively impact improvements in public safety.

Importance of Embedding Cyber Risk Protections in the Early Stages of AV Testing and Deployment

After-the-fact patches and post-release debugging are problematic compared to robust up-front threat mitigation design. Debugging is subject to human error in execution of an effective patch management system. This fact alone is significant because it partially mutes DOT's main benefit analysis that removing human error in the operation of motor vehicles would result in significant public benefits. Compounding and related to this human error problem is that debugging is reactionary instead of proactive. According to the annual Verizon Data Breach Investigation Report (BDIR)¹ for 2015, 99.9% of data breaches happen at least one year after a specific vulnerability has been made public and proper patch management could easily prevent these problems. As the all-caps margin highlight from page 15 of the report states:

"99.9% OF THE EXPLOITED VULNERABILITIES WERE COMPROMISED MORE THAN A YEAR AFTER THE CVE WAS PUBLISHED."

Also, an after-event debugging is more difficult, less systematic and more expensive. In addition, the public trust in any new technology is always fragile. Even a single incident can have asymmetrical negative impacts on public trust and consumer confidence in AVs. A policy which intentionally encourages adoption of software and hardware design with little or no attention to upfront threat mitigation design and completely relies on patching later problems is unwise. In fact, such an approach may largely diminish the essential premise that the number of deaths, injuries and property damage will be reduced by AVs and AV infrastructure build-out. Such an approach is at variance with generally-accepted best industry practices.

Rajant recommends that cyber risk protections be embedded into ADSs at the design and testing stage.

Conclusion

Rajant fully supports the efforts of NHTSA to assist in the development of the AV industry and the safety, technological and social benefits that a well-developed, safe industry could provide. We also support the removal of unnecessary and antiquated rules and regulations. Rajant believes that NHTSA and US DOT must include robust cybersecurity and cyber risk protections as a required part of any pilot program.

Thank you for the opportunity to comment on the possible NHTSA pilot testing program for Automated Vehicles. We are confident that the Agency will move forward with a robust and

¹ The DBIR is recognized as an authoritative source of research on the threat landscape across industries and the world. See 2015 DBIR at p. 15: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf



comprehensive program which will advance this important new technology. Rajant Corporation is prepared to assist with any further information the Agency requests.

Submitted Respectfully,

A handwritten signature in blue ink, appearing to read "Robert J. Schena". The signature is fluid and cursive, written over the printed name and title.

Robert J. Schena
Chief Executive Officer
Rajant Corporation