Western Digital

Western Digital
5601 Great Oaks Parkway
San Jose, California 95119

July 29, 2019

National Highway Traffic Safety Administration
ATTN: Heidi Renate King, Deputy Administrator
U.S. Department of Transportation
Room W12-140
1200 New Jersey Avenue, S.E.
Washington, DC 20590

Submitted via Federal eRulemaking Portal

Re: Advance Notice of Proposed Rulemaking *Removing Regulatory Barriers for Vehicles with Automated Driving Systems*, Docket No. NHTSA-2019-0036

Dear Ms. King:

Western Digital Corporation ("Western Digital") respectfully submits the comments below in response to NHTSA's Advance Notice of Proposed Rulemaking, Removing Regulatory Barriers for Vehicles with Automated Driving Systems, Docket No. NHTSA-2019-0036 (the "Notice"). The Notice seeks comments on the near- and long-term challenges of testing and verifying compliance with existing crash-avoidance FMVSSs for vehicles with automated driving systems and that lack traditional manual controls.

The Notice touched on several areas related to vehicle data, including, *e.g.,* Questions 26 and 27 "What is the most viable method for securely interfacing an external controller with the ADS–DV (*e.g.,* wireless or physical access)?" and "Could a means of manual control be developed that would allow NHTSA to access the system for compliance testing but not allow unauthorized access that could present a security or safety risk to an ADS–DV?" (2019-11032 at 24444).

As the National Transportation Safety Board (NTSB) has observed, "the collection and dissemination of data to NHTSA, the DOT, and the NTSB when appropriate, is critical to establishing safety" of automated vehicle technologies.[1] The NTSB recommended that the DOT and NHTSA define data parameters so that vehicles capture data sufficient to analyze driver and vehicle performance before and during a crash—and that such data should be readily available to NTSB and NHTSA.[2] As NHTSA also has observed, data relevant to NHTSA investigations currently sometimes may not be available

[1] National Transportation Safety Board December 20, 2018 Comments in response to Notice of Request for Comments: Preparing for the Future of Transportation: Automated Vehicles 3.0 (AV 3.0) (Docket No. DOT-OST-2018-0149), *available at* https://www.regulations.gov/document?D=DOT-OST-2018-0149-0129. *See also* Advance Notice of Proposed Rulemaking: Pilot Program for Collaborative Research on Motor Vehicles With High or Full Driving Automation (Docket No. NHTSA-2018-0092), at 83 Fed. Reg. 50874.

[2] *Id.* at 3, 5.

Western Digital
5601 Great Oaks Parkway
San Jose, California 95119

from event data recorders (depending on the event data recorders and the tools used to read them), and manufacturer data logs may not be immediately available or may require proprietary technology to review.[3]

Western Digital supports NHTSA's goal of developing a comprehensive strategy to update the FMVSSs to reflect new realities of vehicle design, and appreciates the agency's efforts to consider all stakeholders' perspectives when developing proposals to modify the existing FMVSSs, including NHTSA's attention to data-intensive aspects of automated driving systems.

These are issues where Western Digital can offer NHTSA particular insights. Our company is a global leader in developing solutions for data storage infrastructure. We manufacture an expansive portfolio of technologies, storage devices, systems and solutions for commercial applications and for consumers. This includes a proven portfolio of automotive-grade products designed for the requirements of connected and autonomous vehicles.

Data storage is an increasingly important aspect of automated driving systems and of connected vehicles regardless of their level of automation. As vehicles employ an expanded array of sensors and processing capabilities, for example, the quantity of data generated by such vehicles is exponentially higher than in conventional vehicles: on the order of 4 terabytes of data per hour.[4] While much of the data collected and stored in today's motor vehicles relate to navigation or infotainment, the data collected and stored by automated driving systems are part of safety-critical systems responsible for driving the car.[5] There also are increasingly data-intensive over-the-air and machine learning applications.

Western Digital believes that data storage is a critical part of ensuring reliable, safe operation of automated driving systems and connected vehicles, as data will play a central role in supporting testing, validation, and reconstruction and evaluation of safety incidents.

Not all hardware is created equally, and NHTSA should consider the impacts of hardware performance on vehicle safety and on the adequacy of NHTSA's test procedures. As the International Organization for Standardization (ISO) recognized years ago: "With the trend of increasing technological complexity, software content and mechatronic implantation, there are increasing risks from systematic failures and random hardware failures."[6] NHTSA has recognized the importance of reliable electronics to vehicle

---

[3] *See, e.g.,* Crash Research & Analysis, Inc. (2018, January), *Special Crash Investigations: On-Site Automated Driver Assistance System Crash Investigation of the 2015 Tesla Model S 70D* (Report No. DOT HS 812 481), Washington, DC: National Highway Traffic Safety Administration, at 11–12, 23.

[4] *See, e.g.,* John R. Quain, *As Cars Collect More Data, Companies Try to Move It All Faster*, N.Y. Times (Aug. 16, 2018), *available at* https://www.nytimes.com/2018/08/16/business/cars-internal-data-networks.html.

[5] *See* Ann Steffora Mutschler, *Data Storage Issues Grow for Cars*, Semiconductor Engineering (Feb. 2, 2017), *available at* https://semiengineering.com/data-issues-grow-for-cars/.

[6] Int'l Organization for Standardization, ISO 26262-6 at vi (rev. Dec. 2018).

Western Digital
5601 Great Oaks Parkway
San Jose, California 95119

safety, and it encourages automakers to adopt engineering safety standards to design electronic systems that can withstand the stresses to which motor vehicles are routinely exposed.[7]

In addition, as automated driving system features become more data-intensive, important questions arise regarding the data collected and how such data should be stored. International standards-making bodies have been working to address such questions. For instance, SAE J1698 (relating to event data recorders) presents standards for time and speed of recording particular types of data (*e.g.*, acceleration or brake pedal position).[8] And ISO 14296 (related to map databases in intelligent transport systems) specifies the format and structure of graphics data.[9]

Developing standards are important not only for ensuring vehicle quality, but also for testing and validation of FMVSS compliance and for accident reconstruction. For example, EDRs can provide a valuable source of data for evaluating the causes of accidents, but they store limited information that may not include all aspects that would be helpful to address how automated driving systems function, such as camera or 3D mapping data or a record of object detection and response.[10] As automated driving systems and connected vehicles progress, it's important to create the right data storage environments, from local storage to the cloud.

Western Digital suggests that as NHTSA updates existing FMVSS related to crash-avoidance—and as it creates new FMVSS related to automated driving systems and connected vehicles— NHTSA should consider data storage requirements, including the following aspects:

- *Memory speed and access.* Automated driving systems require quick access to large volumes of data and computing power. Processing speed may be dependent on memory speed, and slower memory can create latency that could create safety risks in automated vehicles.[11] In addition, system performance is affected by the number of processes running at one time. Where safety-critical processes like an automated driving system share computing resources with nonessential processes like an infotainment system, it is possible for the nonessential process to interfere with a safety-critical process's access to CPU and memory.[12]

---

[7] Nat'l Highway Traffic Safety Admin., *Assessment of Safety Standards for Automotive Electronic Control Systems* (June 2016), *available at* https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/812285_electronicsreliabilityreport.pdf.

[8] SAE J1698-1 at 4.1, 7.1.4, 7.1.11, 7.4-49.

[9] ISO 14296 at 7.3.2.1-7.3.2.2.

[10] *See, e.g.,* 49 C.F.R § 563.7 (specifying data elements collected by EDRs).

[11] *See* Mutschler, *supra* note 5 (noting need for fast memory "to continuously update real time maps" in fully automated vehicles).

[12] ISO 26262 apparently recognizes this risk in requiring estimations of "required resources" for software, including the required "storage space." ISO 26262-6 § 7.4.13.

Western Digital
5601 Great Oaks Parkway
San Jose, California 95119

- *Data integrity.* Stored data can be corrupted through component aging or other factors. For safety-critical processes, it is important to implement "failsafe techniques" that preserve the integrity of data that is central to the system's proper functioning.[13] Some of these techniques may call for duplicating data in different locations, which magnifies the need for data storage.[14] "To address the size requirements, data values can be partitioned into safety-critical data and non-safety-critical data."[15] And "the more safety critical the application, the more unsafe faults must be mitigated."[16] For automated vehicles to be reliable and safe, their automated driving systems must employ data storage that ensures data integrity.

- *Storage capacity.* A related and crucial aspect of performance is amount of storage to which an automated driving system has access. Data storage for safety-critical driving tasks may require multiple backups of data to ensure high reliability,[17] which in turn increases the memory requirements of the system. Western Digital estimates that by 2022, an automated driving system will need multiple terabytes of storage to ensure reliable operation. Automated vehicle developers are currently developing a range of data storage environments, which to varying degrees employ both local and edge-to-cloud solutions. While there may be no one-size-fits-all approach to data storage, the principle remains that storage capacity directly impacts the performance and reliability of automated driving systems.

- *Data segregation; local versus cloud storage.* Many automated driving systems and connected vehicles will rely to some extent on data stored or processing in the cloud. Such distributed computing solutions raise separate issues of cybersecurity and connectivity,[18] and how data should be segregated as part of fail-safe design.

Western Digital recognizes that different automated driving systems may call for different requirements in different systems, and that multiple approaches to data storage may be effective, reliable, and safe. Thus far, however, little attention has been given to the role of data storage in automated driving system performance, safety, security, testing, validation, and incident reconstruction. Western Digital

---

[13] *See generally* Leaphart et al., *Survey of Software Failsafe Techniques for Safety-Critical Automotive Application*, SAE Technical Paper series 2005-01-0779, *available at* https://pdfs.semanticscholar.org/c839/4dcf980b44bdb243ec178ac9b87df2ac6953.pdf.

[14] *Id.* at 3–4 (discussing techniques that preserve integrity of data but which use up more memory space)

[15] *Id.* at 3.

[16] Andrew Hopkins, *The Functional Safety Imperative in Automotive Design*, ARM White Paper at 3 (Sept. 2016), *available at* https://www.arm.com/files/pdf/The_Functional_Safety_Imperative_in_Automotive_Design.pdf.

[17] *See* April Slattery, *Data is the driving force behind autonomous cars - so what about storage?*, Computer Business Review (Oct. 11, 2017), https://www.cbronline.com/storage/data-driving-force-behind-autonomous-cars-storage/.

[18] *See generally 6 Key Connectivity Requirements of Autonomous Driving*, IEEE Spectrum, https://spectrum.ieee.org/transportation/advanced-cars/6-key-connectivity-requirements-of-autonomous-driving.

Western Digital
5601 Great Oaks Parkway
San Jose, California 95119

suggests that NHTSA consider further study, research, and public comment on this important topic.

* * *

Western Digital thanks NHTSA for the opportunity to provide these comments. We hope our comments will assist NHTSA as it considers future rulemaking, and we look forward to future opportunities to contribute.

Respectfully Submitted,

Salman Alam
Assistant General Counsel
Product Regulatory