SAFETY RESEARCH
& STRATEGIES, INC.
340 Anawan Street / Suite 200
Rehoboth, MA 02769
Ph. 508-252-2333, Fax 508-252-3137
www.safetyresearch.net

July 29, 2019

Heidi King
Deputy Administrator
National Highway Traffic Safety Administration
West Building, Ground Floor, Room W12–
140, 1200 New Jersey Avenue SE,
Washington, DC, 20590–0001

RE: NHTSA Docket 2019-036 Removing Regulatory Barriers for Vehicles with Automated Driving Systems

Dear Ms. King:

We are submitting these comments in response to NHTSA's Advance Notice of Proposed Rulemaking regarding the removal of regulatory barriers for vehicles with automated driving systems.

Safety Research & Strategies (SRS) is a multi-disciplined group specializing in product safety, with particular expertise in motor vehicle issues. Our company examines hundreds of vehicle-related death and injury crashes each year. We also examine technology and data and develop strategies and solutions for addressing harm caused by potentially defective products and practices for a wide range of clients including attorneys, engineers, supplier and technology companies and government. We are also regular and frequent advocates for improved safety and consumer protection, providing a significant portion our time *pro bono* to individuals, non-profits, and others who share our interest in advancing safety.

We recognize that many of the current Federal Motor Vehicle Safety Standards were written a half-century ago or more, to regulate vehicles designed and built to be paired with human operators in order to function. And, we can appreciate the agency's desire to prepare for the era in which the human operator may become superfluous. But we are concerned that NHTSA is not promulgating foundational regulations during what will be a long period of semi-autonomy, thereby further widening the gap between the minimum required safety and manufacturers voluntary standards. Missing these foundational steps

and allowing guidance-only standards during this critical time will have a deleterious effect for the public as well as the agency.

There are three key areas of particular concern that have been neglected by the agency that will undoubtedly affect future regulations associated with fully autonomous vehicles: the lack of functional safety standards for critical vehicle controls; the lack of updated standards on the human-machine interface (HMI) of vehicle controls; and the lack of accessible data and interpretation tools to adequately monitor and identify vehicle systems for potential malfunctions.

Lack of Functional Safety Requirements

Electronics remain a largely unregulated area of vehicle safety, even as they dominate vehicle systems fleetwide and the agency pushes forward on autonomous vehicle strategies. The effects of NHTSA's failure to adequately regulate current vehicles and their advanced electronic systems are already having significant impacts on motorists as well as pedestrians and others who are unwitting victims of failed vehicle control systems. The lack of a functional safety requirement for the critical electronic controls that process driver inputs, along with hundreds of other datapoints, in order to make decisions about acceleration, braking and steering, has resulted in designs that are causing crashes and removing the driver's ability to adequately control the vehicle in the event of a component failure.

Functional safety entails eliminating or reducing unreasonable risks to individuals caused by the potential malfunction of electronic or electrical components. It focuses on the risks arising from random hardware faults as well as systematic faults in system design, hardware and software development or in production. In automobiles, this applies to safety systems that prevent crashes, such as mandated Electronic Stability Control (ESC) or anti-lock brakes (ABS), as well as to restraint systems such as airbags, which react post-crash to mitigate crash injuries.[1]

While NHTSA has established regulations involving electronic systems, like FMVSS 126, which requires light vehicles to be equipped with Electronic Stability Control systems, it has not established a functional safety standard that would ensure that electronic components are designed and manufactured to fail safely. For example, in April 2010, General Motors recalled 40,000 Corvette vehicles from the 2004 and 2005 model years equipped with tilt and telescoping steering columns because a malfunction in the Steering Wheel Position Sensor could corrupt the signals in the vehicle's Electronic Stability Control system causing it to apply the brakes to one or more rear wheels.[2] This unexpected braking could put the vehicle into a spin. In this instance, a steering sensor did not fail safely. Instead, the design allowed a sensor signal to activate the eletromechanical brakes causing unexpected and dangerous vehicle behavior that the

[1] Executive Summary Functional Safety in Accordance with ISO 26262; ZVEI German Electrical and Electronics Manufacturers Association; Electronic Components and Systems Division; 2012
[2] Recall 10V172; Notice of Defect and Noncompliance; General Motors, April 26, 2012

driver is called upon to correct in an emergency situation. There are a number of other recalls and Technical Service Bulletins that exemplify similar scenarios.

Rather than regulating functional safety, it appears that NHTSA is content with an industry developed a voluntary standard, ISO 26262.[3] While ISO 26262 may serve as a model for an FMVSS, without codifying a requirement, the standard remains voluntary.

NHTSA should be looking at functional safety in much the same way it designates regulations – at all stages of the failure process:

- Pre-Failure: Component level and component interaction testing, certification and ratings.
- At-Failure: Ensuring minimum levels of failsafe for safety critical electronic deigns.
- Post-Failure: Electronic data recorders for crash data as well as control systems diagnostic data, surveillance of safety data, and examination of past investigations to avoid repeating mistakes and improve outcomes of countermeasures.

HMI Concerns

We have seen how human-machine interface changes, absent regulation, or under an inadequate regulation that doesn't preserve the safety intent, expects drivers to instantly change long-ingrained behaviors, or encourages them to step away from the vehicle's basic operational tasks for a few moments, or intermittently, or only in emergency situations. A poorly designed human-machine interface combined with new technology can be an unfortunate recipe for injuries and deaths. The May 2016 death of Joshua Brown, a Tesla enthusiast who was driving his Tesla Model S in Autopilot mode when it crashed into an 18-wheel tractor-trailer truck that was turning left in front of it on US 27A, west of Williston, Florida, is a good example.

The advent of keyless ignition vehicles with push button Start/Stop is another example. Both owner experiences and litigation made it clear that the marriage of electronics with ignitions and locks resulted in unintended consequences: carbon monoxide poisoning, rollaway crashes and easy thefts – hazard scenarios that were previously eliminated under the FMVSS 114 *Theft Protection and Rollaway Prevention* requirements applicable to traditional metal keys. The standard mandated that the key removal from the ignition cylinder could occur only when the vehicle ignition was in the OFF position and the transmission was locked in Park. However, with the introduction of keyless ignitions, NHTSA redefined the "key" to accommodate aspects of this convenience feature without ensuring that the same safety protections were afforded to drivers with the new technology.[4] As a result, the regulations enabled manufacturers to introduce technically compliant designs that failed to meet the true intent of the standard, which was to

[3] International Organization for Standardization; ISO 26262-1:2018 Road Vehicles – Functional Safety
[4] NHTSA Final Rule; Docket 2005-22093; 91 FR 17755; April 7, 2006

discourage drivers from leaving their keys in the ignition and to minimize the chances drivers would exit their vehicle with the transmission not locked in Park.

Most manufacturers refer to the keyless ignition fobs as the "key," which functions as a proximity device allowing drivers to start the engine when the fob is inside of the vehicle. However, the fob is not the key – the key is an invisible code that is transmitted from the fob to an electronic control unit in the vehicle, which then allows the drivers to push a button to start the engine. Rather, the fob, the physical device that is assumed to be the key, is a *one-way proximity device* and it plays no role in shutting off the engine like a traditional key. This change not only upends the decades of driver interaction with standardized systems that included safety features to minimize unintended consequences, but it presents an illogical operational condition to drivers who know their vehicle can only be started with the fob inside the vehicle but do not know or cannot reasonably be expected to intuit that the reverse is not true.

Many keyless ignition designs allow the driver to exit the vehicle, key fob in hand, with the engine running and the vehicle transmission not locked in Park (with the engine on or off). Combined with increasingly quiet engines and a range of features that remain active for some minutes even when the engine is off – like headlights, infotainment systems and instrument panel lighting – drivers can leave a vehicle, travel great distances from the vehicle with the key fob while the engine is running, and leave the transmission in a non-Park gear without being aware that they have done so.

Rollaway hazards and vehicle theft protection concerns were the basis for FMVSS 114, which prevented key removal from the vehicle ignition cylinder unless it was in the full OFF position and the transmission was locked in Park. Thus, the standard set a minimum requirement that led to designs that provided positive assurance to the driver who exited their vehicle with their key in hand that two things were true: The engine was off, and the transmission was locked in Park. Neither one of these is necessarily true when drivers exit a keyless ignition vehicle with the key fob. In fact, NHTSA's redefinition of the "key," which was an attempt to update FMVSS 114 and accommodate new technology, not only failed to ensure that the same safety protections that formed the intent of the standard were met, but it also it resulted in manufacturers creating scenarios that while technically compliant reintroduced the very hazards the standard intended to eliminate.[5] [6]

Another example of the gap between technology and the human-machine interface is automakers' migration to electronic shifters, some with unconventional shifting mechanisms including monostable designs, rotary knobs, and push buttons. The functional operations of the keyless ignition, combined with the multitude of

[5] The Persistence of Rollaway; The Safety Record; July 24, 2018; http://www.safetyresearch.net/blog/articles/persistence-rollaway or GM Quietly Installs Keyless Engine Shutoff; March 2, 2018 http://www.safetyresearch.net/blog/articles/general-motors-quietly-installs-keyless-engine-shutoff

[6] GM Quietly Installs Keyless Engine Shutoff; March 2, 2018; http://www.safetyresearch.net/blog/articles/general-motors-quietly-installs-keyless-engine-shutoff

unconventional, non-standard e-shift controls that lack the traditional PRNDL (Park-Reverse-Neutral-Drive-Low) configuration – and also lack the tactile feedback provided from a mechanical detent – enhance the likelihood that a driver may not lock the shift control in Park before exiting.[7] [8] [9]

Many designs enhance the likelihood drivers will shift into a position that was not intended based on counterintuitive designs or designs that may appear to function like a traditional PRNDL but don't. Some automakers' vehicles with keyless ignition and e-shifters provide safety features to automatically lock the transmission in Park under certain scenarios or prevent engine shut down if the driver attempts to shut off the engine or exit the vehicle without shifting into Park. The lack of standardization of these controls and features increases the likelihood of injuries and deaths associated with these systems.

It is also notable that some automakers have recalled models with e-shifters to add the software needed to enable an automatic Park application. For example, in 2016 FCA recalled certain Jeep and Chrysler models with the monostable e-shift control to add its AutoPark software,[10] which the company describes as: "an enhanced securement strategy which places the vehicle in "PARK" if the driver attempts to exit the vehicle before placing the rotary gear shift selector in the "PARK" position." In 2018, FCA launched a series of Customer Satisfaction campaigns to add AutoPark to 2014-2017 Dodge and Chrysler models with rotary-style e-shifters.[11] [12]

Finally, we challenge the basic premise of this Notice – that the human occupants of the fully automated vehicle will never play a role in its operation. As the agency points out, General Motors, in its petition for standards relief "categorized what they described as 'human-driver-based requirements' into three categories: (1) Features designed to interface with a human driver, such as manual controls; (2) features designed to provide human drivers with information, such a telltales and indicator lamps; and (3) features to protect human occupants, such as air bags. GM's contention is that its ADS–DVs without traditional manual controls require only the third category of requirements."[13]

This is not true or advisable. And, we do not have to go very far into the past to find examples of technology failures that included NHTSA-acknowledged regulatory

---

[7] Field study investigating gear shifter usability in car rental scenario; Sanna Lohilahti Bladfält*, Camilla Grane and Jon Friström; Pg. 48th Annual Conference of the Nordic Ergonomics and Human Factors Society's (NES) NES2016 –Ergonomics in Theory and Practice; 2016

[8] SBW Feedback -Design of feedback system for increased usability in monostable SBW shifters; Tanya Alvarez Cabrera; Luleå University of Technology; 2017

[9] Gear Shifter Design – Lack of Dedicated Positions and the Contribution to Cognitive Load and Inattention; Sanna Lohilahti Bladfält, Camilla Grane, and Peter Bengtsson; Luleå University of Technology; 2019

[10] Recall 16V240; Part 573 Notice of Defect and Noncompliance; FCA; August 9, 2016

CC[11] Customer Satisfaction Notification UO6 AutoPark Functionality; FCA; May 2018

[12] Customer Satisfaction Notification UO5 AutoPark Functionality; FCA; July 2018

[13] Safety Petition Submitted by General Motors; Petition under 49 U.S.C. § 30113 and 49 C.F.R. Part 555 to advance safety and zero emission vehicles through technology that achieves the safety purpose of the FMVSS; January 11, 2018

response. In 2011, the agency cited Toyota unintended acceleration incidents and the inability of drivers to effectively stop a runaway keyless ignition vehicle as a rationale for amending FMVSS 114 to require a 500 millisecond button press time to stop the engine, "believing it will be long enough to guard against inadvertent shut down, while also short enough for drivers to tolerate for everyday normal stationary shut down."[14] The Notice of Proposed Rulemaking included the conclusions of the investigative report into the August 2009 crash in Santee, California, that resulted in four deaths:

> Push Button Ignition Start with no Emergency Instantaneous Shut off Device—In the event that this vehicle was producing unwanted power, there was no ignition key that could be mechanically actuated to instantaneously disconnect electrical power to the engine. In place of the key is a software push button that delays engine shutdown for three seconds once depressed. This instruction is not indicated on the dashboard.[15]

Autonomous technology will fail, and those malfunctions will initiate a response from the human occupants. Will they attempt to exit the vehicle? Will they be able to shut down the vehicle? These are but a couple of obvious scenarios not contemplated in the current ANPRM, nor in the current guidance.

As long as humans are in the vehicle, there will be a need for vehicle controls of some type. In fact, the age of full vehicle autonomy is going to require a thorough and thought-out HMI strategy. Ignoring this critical aspect of automotive safety during the transition to complete automation will make the development and implementation of such a strategy more difficult.

Data Accessibility and Interpretation

As the vehicle takes over most of the operational functions, the amount of data it must gather, assess, and store, and the speed at which it must process this information will increase exponentially. Indeed, that is already happening – autonomous test vehicles "typically generate between 5TB and 20TB of data per day, per vehicle."[16] Even in current Level 2 vehicles the amount of data that is transmitted between modules, which is stored to widely varying degrees amongst vehicles, is extraordinary, and the tools available to the public, law enforcement and diagnosticians are generally limited to OBD II diagnostic scans and Event Data Recorders. This leads to the inability to independently examine, document and identify potential vehicle-related failures and can and does result in motorists' being charged civilly and criminally for at-fault crashes without the ability to properly defend themselves. Despite the plethora of data circulating in a vehicle that can be used to identify potential vehicle defects, it may not be recorded unless a preset

[14] Docket 2011-0174; Notice of Proposed Rulemaking 76 FR 77178; National Highway Traffic Safety Administration; December 12, 2011.
[15] Docket 2011-0174; Notice of Proposed Rulemaking 76 FR 77178; National Highway Traffic Safety Administration; December 12, 2011.
[16] Data storage is the key to autonomous vehicles' future; Mark Pastor; ioTNow Transport; February 14, 2019

active fault is flagged. Further, the publicly available tools used to examine the vehicle and driver behavior, which include OBD II diagnostic scanners and scan tools to extract the Event Data Recorder, are able to access only a fraction of what may be needed or available to the manufacturer.

Presumably, failures in fully autonomous vehicles will not lead to at-fault charges of occupants who have no controls; however, establishing a framework for data accessibility and interpretation that is not reliant on the manufacturer as the sole arbiter as to its meaning will be important for accountability and public acceptance. The need to address this is immediate and it should be part of the suite of rulemakings that NHTSA prioritizes and should include current vehicles.

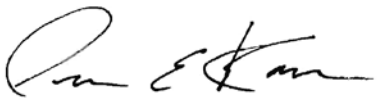
The Diagnostic Trouble Codes (DTC) relied on to identify potential causes of vehicle malfunctions are an outgrowth of a 1995 U.S. Environmental Protection Agency (EPA) Final Rule regarding On-Board Diagnostics.[17] In the current age of semi-autonomous vehicles, they do not provide the granular detail necessary and are fast becoming relics.

Likewise, Event Data Recorders, while helpful, are also crude gatherers of limited vehicle pre-crash and crash metrics that store limited data at sampling speeds far slower than is adequate to understand the complete vehicle and driver behavior leading up to and during a crash.

The rights of motorists as well as NHTSA ‘s ability to understand potential vehicle defects is greatly hampered without clear data accessibility requirements and accessible interpretation tools.

In conclusion, we recommend that NHTSA approach this technological sea change by returning to its roots as a public health agency, taking the epidemiological approach to injury control that has proven successful in tracking and mitigating biological threats that continue to change, much like the technology in motor vehicles.

Sincerely,



Sean E. Kane

[17] Control of Air Pollution From New Motor Vehicles and New Motor Vehicle Engines; Regulations Requiring Availability of Information for Use of On-Board Diagnostic Systems and Emission-Related Repairs on 1994 and later Model Year Light-Duty Vehicles and Light-Duty Trucks; 60 FR 40474; U.S. Environmental Protection Agency; August 9, 1995