NOV 2, 2021 1 MIN READ OPINION

When Teslas Crash, ‘Uh-Oh’ Is Not Enough

Today’s regulatory structure has given Tesla license to peddle the illusion of self-driving and tout its beta software experiments on public roads as a breakthrough in automotive technology.

By **Junko Yoshida**

What’s at stake?
Tesla’s autonomous-vehicle strategy is about to become a playbook for the broader automotive industry on sidestepping the National Transportation Safety Board’s safety recommendations and bending the prior administration’s toothless AV regulations to its will. But when Tesla’s Full Self-Driving beta software kills a pedestrian, regulators must do more than say, “Uh-oh”; they must get to the bottom of what went wrong. That requires a deep dive into the software — a task for which regulators today are ill-equipped. Ensuring the public safety requires rewriting the rules and arming the regulators to enforce them.

Tesla, whose market cap now tops $1 trillion, merits recognition for defying every technology and business shibboleth of the traditional auto industry.

But its reckless behavior on public roads must likewise redound to the automaker’s reputation — and reverberate through the regulatory bodies charged with ensuring the safety of autonomous vehicles and protecting other road users.

Tesla CEO Elon Musk and his myriad minions revel in taunting everything and everyone. A recent target has been National Highway Traffic Safety Administration’s new senior safety adviser, Missy Cummings. The Duke University professor and former fighter pilot was bullied off Twitter within days of her NHTSA appointment last month.

By egging on its fans, Tesla has perpetuated the illusion that it can do no wrong. But there has already been disturbing evidence to the contrary. And when its beta software inevitably injures someone, fresh doubts about Tesla-tech will seed misgivings about the pot of gold at the end of Musk's autonomous-driving rainbow.

It's time for the feds to rein in Tesla, but not by targeting Tesla alone. NHTSA must develop the software savvy to trace vehicle failures that start not with the driver or with a mechanical problem but somewhere deep inside all those ones and zeroes. NHTSA must become an effective evangelist for proactive automotive safety. It's time for NHTSA 2.0.

Easier said than done

The problem is that NHTSA historically has focused on mechanical systems.

"Mechanical failures are easy to identify, and a recall can be ordered," noted Colin Barnden, principal analyst at Semicast Research. But "NHTSA has never really mastered electronics and the proliferation of ECUs and networks — CAN, LIN, etc. — in the vehicle.

"Software defects, such as [Toyota's] unintended acceleration, are not so easily identifiable, and NHTSA has found even this difficult," he added

As the industry enters a "new world of software-defined cars, neural nets, machine learning and over-the-air updates where an automaker can make whatever changes it likes without telling anyone, NHTSA has been exposed as completely out of its depth," said Barnden.

Ending the 'driver error narrative'

Phil Koopman, an associate professor at Carnegie-Mellon University with expertise in verifying autonomous systems, took the NHTSA's "driver error narrative" to task in a 2018 paper on **automotive safety practices**. "In a sense, NHTSA got caught napping on software safety by autonomous vehicle technology," Koopman told us.

Crash investigations — both by NHTSA and by OEMs handling complaints — "typically presume driver error without ruling in potential software defects," said Koopman.

"NHTSA has not staffed up on computer system safety," Koopman said, because "if you essentially never blame the computer software for a crash, there's no apparent need to hire staff with special expertise and training in dealing with software issues."

Automakers and regulators must recognize that when vehicle autonomy removes the human driver from the equation, "the whole story must change," cautioned Koopman. In a highly automated vehicle, the driver is the software running on the computer system. Without a human to blame for accidents, "software safety" should become the primary concern for investigators, Koopman said.

Tesla's offenses

Although not the whole story, Tesla's behavior to date makes a clear case for consequential changes in NHTSA's regulatory oversight of advanced driver-assistance systems (ADAS) and AVs. Tesla's offenses include:

— releasing its unfinished Full Self-Driving beta software on city streets with untrained drivers;

— blatantly ignoring recommendations issued by the NTSB after numerous investigations of Tesla crashes;

— exploiting "**L2 loopholes**" (to avoid more stringent AV oversight, Tesla describes its vehicle as SAE Level 2, despite its design intent for Level 4 autonomy) ;

— pushing safety-related software updates without telling anyone

— taking no action to prevent consumers' potential misuse of the vehicle's Autopilot; and

— pitching its non-AV cars to consumers as fully self-driving.

Against this backdrop, safety experts, industry observers, and media are increasingly critical of Tesla's misbehavior.

Last week, Koopman tweeted **video footage** of a Tesla under automated control as it roars through a stop sign without intervention by its test driver.

“This is both a defective product (an AV that ignores stop signs), and reasonably foreseeable misuse (driver did not intervene because this was “testing”), Koopman tweeted, imploring NHTSA to “intervene before the seemingly inevitable fatalities occur.”

Phil Magney, founder of VSI Labs, often calls Tesla “a proxy for future vehicles.” Problems evident in Tesla’s practices, left unchecked, will become precedents followed by the entire automotive industry. “It is my belief that NHTSA has recognized that traditional OEMs are following in Tesla’s path and strive to do the same thing,” Magney said. This obligates the agency “to do something” quickly.

Regulations coming down the pike

What are the AV and ADAS regulations that could — or should — be in development or under consideration at NHTSA 2.0? The Ojo-Yoshida Report asked industry experts what they want NHTSA 2.0 to consider.

1. ODD enforcement

Topping the list is enforcement of stricter operational design domains (ODDs) for highly automated vehicles.

“Most would agree, I believe, that automated driving systems, regardless of automation level, should be confined to areas that are vetted,” said Magney.

Certain issues can be defined in advance as problematic for automated driving systems. “It might be something about the geography of the road, the quality of the road surface, the readability of lane markings, the exposure to humans, and vulnerable road users,” Magney said. Carmakers and regulators should identify those areas, mark them as “problematic,” and remove them from the ODD, he said.

Koopman’s proposed “starting point” is “a shared repository of potential hazards that must be addressed.”

Barnden went so far as to propose that NHTSA “ban the use of Level 2 partial automation systems in proximity to vulnerable road users such as cyclists and pedestrians.” He called for creation of a federally designated ODD that would describe “precisely where Level 2 partial automation can be activated” and predicted that, “based on safety recommendations from NTSB following multiple

fatal Tesla crashes, this is certain to be divided highways only for the foreseeable future."

If enacted, the proposed ODD would corral Tesla's Autopilot and Full Self-Driving (FSD), as well as GM Ultra Cruise, into "limited-access environments away from urban settings," said Barnden.

2. Responsible road testing
Road testing must come with clear guidelines, the experts told us.

Historically, the car industry behaved in a generally responsible manner when testing vehicles on public roads, Magney noted. That changed when Tesla deployed its FSD beta software.

Today, the rules for vehicle testing on public roads are based on SAE J3016, which laid out the taxonomy — the familiar Levels 1–5 — for categorizing driving system autonomy. In a regulation-evading maneuver now known as the Level 2 loophole, Tesla found a way to exploit SAE J3016 definitions to deploy an early Level 4 prototype on public roads but bill it as Level 2, so that the human driver bore the ultimate responsibility for the car's behavior.

Koopman therefore proposes that regulators abandon SAE J3016 as the benchmark for deciding which vehicles can be tested on public roads under what conditions. Instead, regulators should ask: Is the car in question a vehicle automation test platform or a mature, deployed product? By this standard, a Tesla controlled by FSD beta software is a "test platform," Koopman said, because a human test driver — whose skills must exceed those of a typical driver — is expected to compensate for hazards caused by the AV's misbehavior.

Barnden made a more drastic proposal: "NHTSA should declare an immediate operation and testing moratorium for Level 4 high automation on public roads." The agency should "engage with the developers, operators, and other stakeholders — such as NTSB. safetyu advocacy groups, cycling safety advocates, etc. — to provide unambiguous answers to the questions of safe testing and safe operation," he said.

Recognizing that these are thorny questions, Barnden said, “I applaud NHTSA for appointing Missy Cummings, who is the undisputed expert on these matters. I’d like to see Phil Koopman take up a safety advisory role too.”

3. Test-based approach to safety case
In validating safety for computer-based vehicles that depend on software, testing is necessary but insufficient. “Testing doesn’t make you safe,” said Koopman.

He wants to see NHTSA “transition from its current test-based posture to a safety case-based approach that includes testing as a component.”

A safety case-based approach would require NHTSA to ask highly automated vehicle makers to use safety cases in which they (a) define what they mean by safe, (b) explain the reasoning behind their safety claims, and (c) provide tangible evidence that supports their reasoning, Koopman explained.

4. Clear rules on responsibility
NHTSA must clarify the responsibilities of human and machine drivers.

“NHTSA needs to understand that there are two roles technology can play to save lives on public roads,” said Barnden. One is to make humans into safer drivers. Another is to replace humans as drivers.

“NHTSA needs a twin-track approach to immediately advance a mandate for proven safety technology — automatic emergency braking, lane-keeping systems, driver-monitoring systems, intelligent speed adaptation, back-up assist, blind spot detection — with performance minimums for each one),” Barnden said.

Koopman said NHTSA must ensure that “the division of tasks between human operators and automated vehicles results in acceptable safety.” This should include “monitoring deployed vehicles for an unsafe division of responsibility — e.g.. systems overly prone to automation complacency that results in elevated mishaps rates — as well as longer-term research into driver-monitoring effectiveness at ensuring operational safety.”

Further, NHTSA should encourage the industry “to develop standards for measuring driver engagement in the context of driver-monitoring systems and their effectiveness in naturalistic driving situations,” he said.

5. NHTSA's recall policy

Regular over-the-air (OTA) software updates are an established and well-accepted practice for consumer products such as smartphones and cable set-top boxes, but in the automotive world, a recall policy still stands. Changes intended to fix a safety problem must be reported, regardless of whether they are performed at a dealership or via an OTA update.

"However, there is certainly a temptation to skip reporting if a stealth recall can be snuck into a weekly update," said Koopman. "NHTSA might need to require routine reporting of all updates with a manifest that identifies safety-relevant changes."

There are other concerns. What if an OEM insists its vehicle is exempt from recall reporting because it's a "test" platform?

Koopman said, "If non-employee civilian drivers are operating 'test' software, that software should be subject to … recall."

6. Conformance to industry standards

NHTSA should embrace industry standards and insist that automakers conform.

This mandate is critical, Koopman said, because the standards were written by the automotive industry and stakeholders themselves. They were issued as normative standards by accredited organizations, including the ISO, ANSI/UL, and SAE). The list of applicable standards includes but is not limited to ISO 26262, ISO 21448, ANSI/UL 4600, and safety-relevant security standards, Koopman noted.

Koopman also would like to see NHTSA ask automakers to include full self-disclosure of standards conformance status for every highly automated vehicle on the road. If no safety standards are followed, he said, the automaker should say so.

Further, he said, NHTSA should ask for a clear compliance statement — "We conform to ISO 26262," for example. Evasive language such as "We use approaches inspired by" a given standard or "We adopt techniques drawn from" a given list of standards should not be accepted.

Conclusion

Today's regulatory structure has given Tesla license to peddle the illusion of self-driving and tout its beta software experiments on public roads as a breakthrough in automotive technology. In response, expect (or hope for) NHTSA to go "2.0" and take a more aggressive, consumer-centered approach to AV regulation.