

Computer-Driven Vehicle (CDV) Operations Regulator Safety Approval Checklistⁱ

Most of us who are impacted by computer drivers don't have the ability to fully vet industry claims about automated vehicles. We made this checklist as an easy-to-use guide to assist regulators and the general public in understanding key safety questions that should be asked about computer driven vehicles, no engineering degree required.

This checklist is a supplement to a full safety evaluation. It is intended help people working on safety regulations craft policies that effectively reduce the risk of harm caused by the auto industry's rush to capitalize on autonomy. In the absence of federal and state standards regulating computer driven vehicles, automakers operate in a regulatory vacuum. When automakers are not subject to firm and enforceable requirements, history has shown us that public safety will be the loser.

By having the AV company, automaker, robotaxi service or another player in the CDV field answer these questions, you'll be able to spot any glaring holes in their safety claims. Those answers will reveal if they've really made public safety a top priority in their claims that they're ready to operate on public roads.

As time and resources allow, additional questions will be added, and references providing further insights into CDV safety will be identified in the end notes.

Definitions:

- Computer-Driven Vehicle (CDV) is any automotive technology that automates driving tasks of sufficiently long duration to potentially allow or induce life- or safety-critical events to threaten, injure, or kill the vehicle's occupants, other motorists, vulnerable road users, or destroy other property. (Includes SAE J3016 Automation Levels 2,3,4, and 5.)ⁱⁱ
- ODD is the set of geographic, temporal, and environmental constraints defining the applicant CDV's authorized operation. (See SAE J3016 for complementary ODD definition.)
- Risk is the combination of consequence of hazard and its likelihood of occurrence. (Note: Either potential consequence of the hazard or its likelihood of occurrence may make the risk unacceptable.)

ID	YES	NO	QUESTION
1			Has the applicant followed a generally accepted process for validating performance and safety of the applicant's CDV technology? ⁱⁱⁱ
2			Has the applicant developed and validated compliance with a comprehensive safety case analysis for its subject CDV private, institutional, or for-hire offering? ^{iv}
3			Has the applicant shown its CDV offering has passed a safety case audit by competent and qualified independent auditors?
4			Has the applicant adequately documented the CDV's ODD?

5		Has the applicant shown that all CDV operations within the ODD are legal? ^v
6		Have all applicable federal, state, regional, and local authorities approved the ODD?
7		Has the applicant received regulatory approval for CDV operation only within the ODD boundaries?
8		Has the applicant shown that the CDV will respond safely if for any reason it is operated outside of its ODD? ^{vi}
9		Has the applicant shown that the subject CDV(s) will promptly and safely comply with emergency modifications of or restrictions to the approved ODD? ^{vii}
10		Has the applicant crash-tested subject CDV(s) to prove post-crash safety of its occupants?
11		Has the applicant disclosed plausible significant CDV operational risks to occupants, vulnerable road users, or property that it has not mitigated? ^{viii}
12		Has the applicant disclosed and shown evidence of risk mitigation for risks it has determined to be plausible, acceptable and reasonable for occupants of the subject CDV? ^{ix}
13		Has the applicant disclosed and shown evidence of risk mitigation for risks it has determined to be plausible, acceptable and reasonable for other motorists, public safety officials, emergency responders, vulnerable road users, and properties outside of the subject CDV?
14		Has the applicant included adequate reasonable physical safeguards and visible/audio warnings to alert and promote self-defense of motorists and other road users outside of the CDV if the CDV exhibits anomalous behavior or if collision is likely or imminent? ^x
15		Has the applicant shown that it will not endanger or injure anyone by its near-term post-collision actions? ^{xi}
16		Has the applicant proven the safety of occupants and other road users in the event of electrical power loss? ^{xii}
17		Has the applicant proven the safety of occupants and other road users in the event of loss of external communications or connectivity, particularly with regard to notification and controlled response to emergency ODD restrictions?
18		Has the applicant shown that CDV operation would not replicate dangerous, injurious, or lethal circumstances for which prior use or other known prior CDV control system, software, perception, or physical configuration have been a factor? ^{xiii}
19		Has the applicant shown that safe disposition of the subject CDV in the event of loss of data processing capability or electronic sensors? ^{xiv}
20		Has the applicant shown that expedited emergency egress on demand is enabled, including in the event of loss of electrical power
21		Has the applicant established that any paying for-hire customer must opt-in to forced mediation if proposed by the applicant or its agents?
22		Has the applicant provided adequate insurance for both occupants and potential external collision victims?

23		Has the applicant shown that the subject CDV cannot be used to deliver dangerous or illicit goods when unaccompanied by a live customer?
24		Has the applicant proved that safe ingress, egress, and expedited egress on demand is available regardless of user's race, sex, physical or mental incapacities?
25		Has the applicant proved that unaccompanied underage users are prohibited from use?
26		Has the applicant designed for and proved that the intended CDV user's destination may be safely and expeditiously modified by its user if in their sole determination the original destination is undesirable or unsafe?
27		Has the applicant proven that CDV commands and redirections are secure, authenticated, and legal?
28		Has the applicant shown that CDV occupants are adequately protected from harassment, entrapment, and threatening actions by unauthorized, unwelcome, or threatening third parties?
29		Has the CDV been certified to comply with all applicable FMVSS requirements?
30		Has the applicant shown that the CDV collects and saves enough operational data to resolve root cause of incidents and collisions?
31		Has the applicant shown that operational data recorded before a reportable incident or collision is preserved and accessible to stakeholders for post incident/crash root cause engineering evaluation and/or legal use by those with direct interest? ^{xv}
32		Has the applicant shown that the subject CDV's conventional mechanical equipment, electrical and electromechanical components, and passive hardware are inspectable by officials during required periodic and on-demand safety inspections? ^{xvi}
33		Has the applicant shown that the subject CDV's safety-critical and life-critical logical functionality operation is inspectable by officials during required periodic and on-demand safety inspections? ^{xvii}
34		Has the applicant shown that safety-critical and life-critical electrical and electronic components are safely within their expected lifetime? ^{xviii}

ⁱ Direct questions and comments to contact@autosafety.org

ⁱⁱ See section 2.3 ff. How Safe is Safe Enough, P. Koopman, 2022; <https://www.amazon.com/How-Safe-Enough-Predicting-Autonomous/dp/B0BCSCZ6NC>, for additional discussion of SAE J3016 automation level definition deficiencies. Also note that SAE J3016 is not a safety-related document and has not been evaluated for its role in public safety.

Also see Embodied AI Safety, P. Koopman, 2025, <https://philkoopman.substack.com/p/my-new-book-embodied-ai-safety> for additional background on hazards and shortcomings of AI reliance for CDV control safety., related keynote address https://open.substack.com/pub/philkoopman/p/keynote-talk-embodied-ai-safety?utm_campaign=post&utm_medium=email

ⁱⁱⁱ See for example Technology Readiness Assessment Guide: Best Practices for Evaluating the Readiness of Technology for Use in Acquisition Programs and Projects [Reissued with revisions on Feb. 11, 2020.], US Government Accountability Office, <https://www.gao.gov/products/gao-20-48g>; <https://www.gao.gov/assets/710/706680.pdf> pg.124, Table 12: Department of Transportation Technology Readiness Levels (2017)

^{iv} See for example UL 4600.

^v <https://www.latimes.com/business/story/2025-10-21/driverless-waymo-taxis-under-investigation-after-failing-to-stop-for-a-school-bus>

^{vi} A CDV could be inadvertently located outside of its ODD by, e.g., sudden weather events, forced diversion, diversion, unplanned delays forcing violation of temporal constraints, etc.

^{vii} Emergency ODD modifications may be directed by authorities in response to emergency actions, construction, unusual events, or mass actions.

^{viii} Risk has two factors, likelihood of occurrence and consequence of occurrence or hazard. The rationale for acceptance of any plausible unmitigated hazard must be justified by convincing explanation of why it is sufficiently unlikely to occur?

^{ix} Many CDV developers use the definition of safety found in ISO 26262, “absence of unreasonable risk”. (Also see ISO 26262; 49 USC § 30102(a)(9); UNECE Inland Transport Committee ;World Forum for Harmonization of Vehicle Regulations; Guidelines and Recommendations for Automated Driving System safety requirements, assessments and test methods to inform regulatory development) It is important to note that the corollary of this definition is that in any real system, a purported safe offering that is absent of unreasonable risk will therefore also have present risks that the developer feels are reasonable. That does not necessarily mean that they would be acceptable to the public. They might fail to adequately consider unacceptably dangerous residual hazards or that their likelihood of occurrence is greater than presumed. Those risks must be disclosed and understood before a CDV offering may be determined to be safe enough for public use.

^x Warnings such as flashing headlights or others, audible alerts, etc. if the CDV is out of control or deviates dangerously from a safe trajectory, or otherwise endangers the public.

^{xi} Note prior events including injury to pedestrian being dragged post-crash, injury to bicyclist caused by CDV discharging passengers in restricted zone, injuries and massive pileup due to phantom braking, and other deaths involving DV operation, etc. have been documented.

^{xii} Loss of electrical power can cause loss of vehicle control, loss of communications, trapping occupants inside of locked vehicles, disabling occupant egress, etc.

^{xiii} Note prior events including computer-driven vehicles causing death of pedestrian walking a bicycle at night, multiple deaths of computer-driven vehicles encountering semi-trailers, death due to misinterpretation of highway exit gore existence and/or signage, injury to pedestrian being dragged underneath a CDV post-crash, injury to bicyclist caused by CDV discharging passengers in restricted zone, injuries and massive pileup due to phantom braking, high speed DV crashes into emergency responders, stationary vehicles including semi-tractor trailers and stationary automobiles, and other deaths involving CDV operation, etc. Consequential incidents are not limited to those identified as ‘at fault’ by applicant or third parties.

^{xiv} Including incapacity or compromise due to cybersecurity breach.

^{xv} As of October 2025, Tesla CDVs are programmed to automatically alter their reported operating state from automatic to manual control when a collision while on automatic control is imminent or occurs, intentionally obscuring the manufacturer’s liability.

^{xvi} Lights, wipers, tires, suspension, brakes, glass, horn, pollution controls, etc

^{xvii} Sensors, data processing equipment, safety margins, data storage, built-in tests and diagnostic results, etc.

^{xviii} Certain components necessary for safe vehicle operation, notably batteries, solid-state memory, and graphical displays, have limited life potentially shorter than the expected lifetime of customary automobile technology,