Motional's Safety Case Framework for Commerical Driverless Operations

2026



Motional

Executive Summary

Driven by a corporate philosophy that places safety above all else, Motional integrates rigorous engineering standards, continuous field management, and transparent governance across every stage of its technology lifecycle. As one of the early pioneers in autonomous driving, Motional has extensive expertise in establishing, refining, and validating comprehensive safety methodologies across all stages of the system development, fleet deployment and operations, and safety management. The combination of Motional's safety-focused culture with industry-leading expertise and experience enables the company to responsibly commercialize autonomous vehicles (AVs).

To promote transparency and the evolution of industry standards on safety, Motional presents our systematic approach to safety with the following Safety Case Framework. This framework articulates the rigorous methodology, structured arguments, and empirical evidence used to evaluate system readiness and demonstrate that the Motional Autonomous Driving System (ADS) operates safely in driverless commercial ride-hail operations. Applied specifically within our Operational Design Domain (ODD) in the dynamic, highly-complex environments that Motional operates[1], this framework provides a clear overview of our structured safety methodologies, showing how Motional IONIQ 5 robotaxis navigate with exceptional behavioral competence and consistent real-world safety.

Our approach addresses three fundamental questions: Are we operating responsibly? Have we designed our vehicles to respond safely when something goes wrong? And can our AVs navigate the roads competently? These questions form the foundation of our three safety pillars: Operate with Responsibility, Architect for Resilience, and Drive with Competency.

Operate with Responsibility. This pillar details how Motional instills a safety-first culture throughout every level of the organization. It encompasses our enterprise-wide Safety Management System (SMS), active risk management processes, internal safety governance bodies such as the Safety Review Board, continuous field monitoring, and close coordination with regulatory agencies and emergency services.

Architect for Resilience. This pillar describes how safety is integrated directly into the physical and technical design of our vehicles and software stack. It explains our automotive-grade platform redundancy, multi-modal sensing systems, redundancy across our autonomous driving architecture, fault-tolerant execution, cybersecurity protections, and systematic responses to unexpected system faults or human misuse.

Drive with Competency. This pillar focuses on the behavioral evaluation of our driving software within the defined ODD. It explains our multi-stage verification and validation pipeline—combining large-scale simulation, closed-course testing, and public road evaluation—alongside advanced collision-avoidance capabilities and post-incident response protocols.

In this paper, Motional details the structural methodologies, technical engineering principles, and operational safety processes that collectively ensure our driverless vehicles operate safely, reliably, and harmoniously with dynamic environments.

---

[1] Motional currently conducts commercial operations in Las Vegas and testing in Pittsburgh. Motional's operational markets are chosen for complex urban environments where there is demand for safe and convenient transportation.

Introduction

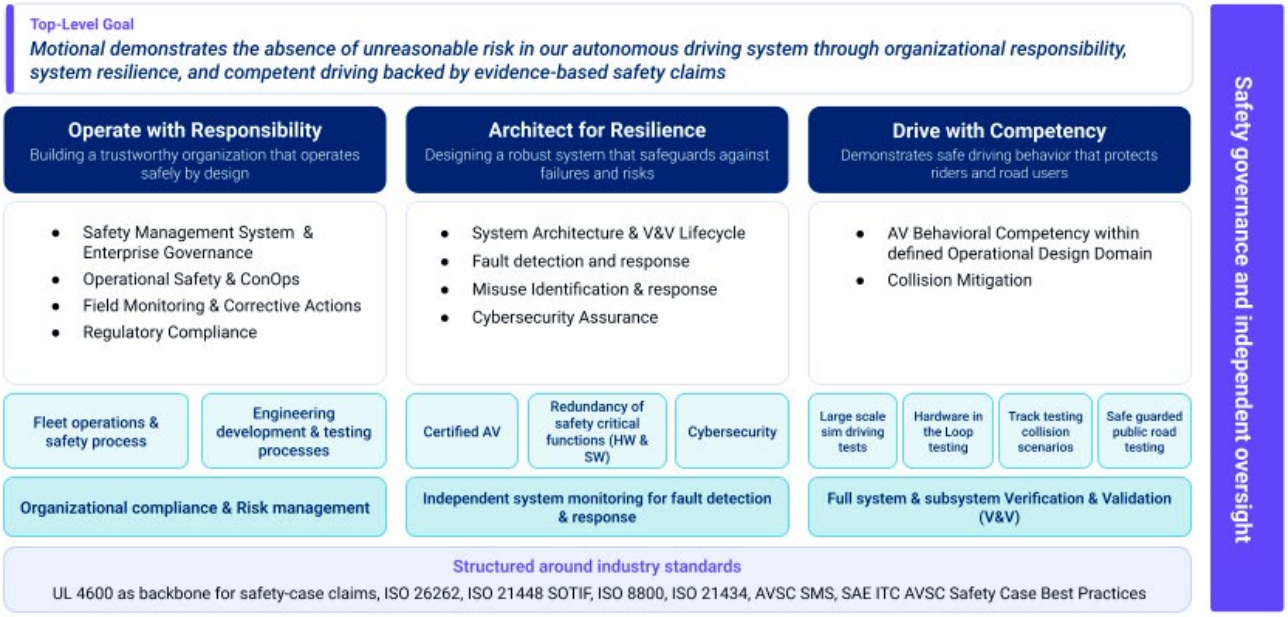
Automated driving technology has entered an era of profound technological progress, offering unprecedented potential to improve road safety and provide new personal mobility choices. Motional brings extensive operational and technical background to this field, backed by over 2.6 million autonomous miles driven across diverse geographic regions and urban topologies, as well as more than 145,000 public passenger trips safely completed on major ride-hailing platforms. As a company, Motional has adhered to the fundamental philosophy that safety cannot be evaluated as an afterthought; rather, safety must be systematically built into every architecture, algorithm, operational policy, and organizational structure.

While there currently is not a federal regulatory framework for Society of Automotive Engineers (SAE) International Level 4 automated driving systems, establishing clear, transparent, and rigorous safety methodologies is vital to building public trust and advancing safety science across the industry. Motional's Safety Case Framework provides a structured, evidence-based argument that aggregates qualitative and quantitative findings to demonstrate that our AV operations achieve an absence of unreasonable risk. A safety case serves as a comprehensive logical framework, articulating top-level safety objectives and linking them directly to concrete design choices, hazard analyses, rigorous testing regimens, and continuous operational evidence.

Motional's framework draws upon foundational safety engineering disciplines established across automotive, aerospace, and robotics domains, synthesizing best practices from published industry standards. The structure of our overarching safety argument is heavily informed by UL 4600 (Standard for Safety for the Evaluation of Autonomous Products), which acknowledges that there is inevitable risk in transportation systems and thus the top-level objective must be to achieve an absence of unreasonable risk. Physical systems functional safety and hardware component reliability evaluations align with ISO 26262, while safety of the intended functionality is evaluated using principles from ISO 21448 (SOTIF). Additionally, Motional actively collaborates with key industry bodies, such as the Automated Vehicle Safety Consortium (AVSC), to contribute to and incorporate emerging consensus standards across autonomous vehicle development.

A foundational premise of modern system safety is that absolute zero risk is unattainable in any real-world road paradigm. Consequently, safety engineering focuses on systematically identifying, evaluating, and mitigating risk to ensure the total avoidance of unreasonable risk. Motional's top-level safety goal translates this principle into actionable engineering and operational practices structured across three interdependent pillars: Operate with Responsibility, Architect for Resilience, and Drive with Competency.

Motional's Safety Case Framework



As illustrated in the framework overview above, the three pillars ensure that organizational accountability, hardware and software resilience, and behavioral proficiency operate to maintain safety across the complete lifecycle of our autonomous driving technology.

Pillar One:
Operate with Responsibility

An autonomous driving system cannot achieve safety through technical software design alone; it requires an organizational foundation steeped in safety culture, systematic oversight, and continuous operational vigilance. Operating with responsibility signifies that Motional instills safety considerations into corporate process, employee training protocol, operational workflow, and managerial decision. This organizational commitment ensures that safety remains paramount across all phases of engineering, testing, and deployment.

Operational Safety and Concept of Operations (ConOps)

Executing safe, scalable fleet operations requires unambiguous, standardized operational procedures that govern routine tasks, preventative maintenance, and emergency response. Motional develops and implements Standard Operating Procedures (SOPs) across all phases of vehicle life. These SOPs define precise operational workflows for vehicle technicians, depot personnel, and fleet managers, ensuring consistent execution, rigorous safety oversight, and repeatable handling of complex operational conditions.

To establish boundaries for safe execution, Motional rigorously defines both the Operational Design Domain (ODD) and the Concept of Operations (ConOps). The ODD explicitly defines the environmental, geographic, roadway, and atmospheric conditions within which the automated driving system is specifically designed to operate.

Complementing the ODD, the ConOps defines how the autonomous vehicle functions within these boundaries, including user interaction models, dispatching rules, passenger safety protocols, and operational support infrastructure. Together, the ODD and ConOps provide clear operational parameters, enabling the system to reliably detect when environmental conditions approach or exceed design boundaries.

Recognizing that dynamic urban road environments occasionally present unusual obstructions, unexpected road closures, or law enforcement directions, Motional incorporates multi-layered operational support systems with humans-in-the-loop. Motional employs highly-trained Remote Vehicle Assistance (RVA) agents to provide contextual guidance or route confirmation when an AV encounters unusual or complex scenarios. Importantly, RVA agents do not remotely steer or control the vehicle; the vehicle's onboard automated system retains full responsibility for path execution, vehicle control, and real-world collision avoidance, and can reject an RVA agent's guidance if needed to ensure safety. In scenarios where a physical presence is required, Motional field recovery teams are deployed to clear obstacles or inspect vehicles directly. Furthermore, Motional mission control specialists continuously monitor fleet status, while passenger assistance mechanisms allow riders to request safe roadside pullovers at any time, ensuring total passenger comfort and operational safety.

Safety Management System (SMS) and Enterprise Governance

Motional's enterprise-wide Safety Management System (SMS) provides the structural framework for identifying hazards, evaluating risks, implementing controls, and systematically measuring safety performance across all business units. Adopting established principles from aviation and transportation safety engineering, our SMS integrates four core components: Safety Policy, Safety Risk Management, Safety Assurance, and Safety Promotion. This structure ensures that safety governance is embedded into engineering design and development, executive decision-making and continuous technical development.

Through our Safety Risk Management (SRM) program, potential hazards are identified systematically during technical design, simulation, track testing, and public road driving. Risks are rigorously evaluated along key quantitative and qualitative dimensions, examining severity, frequency, controllability, and detectability. Identified risks are cataloged within an enterprise Safety Risk Register, where appropriate technical or operational mitigations are designed and tracked. Higher-severity risks are formally escalated to Motional's Safety Review Board (SRB), an executive governance body comprising Motional's senior executive, engineering, and safety leadership, which holds final authority over risk acceptance, software deployment authorization, and policy enforcement.

- **Frequency:** Estimating the statistical likelihood of occurrence within the operating domain.
- **Severity:** Evaluating potential outcomes and potential impact to vehicle occupants and road users.
- **Controllability and Detectability:** Assessing system fail-safe capabilities and detection abilities, as well as whether the autonomous vehicle was the initiator or responder to the situation.

Safety promotion and employee empowerment complement these technical structures. Motional maintains open safety reporting channels and a strict non-retaliation policy, encouraging every employee to raise safety concerns or initiate system reviews. We utilize a 'Red Button' process, which allows team members across the business to "press the Red Button" and initiate an urgent assessment and decision on the safety issue reported. This can result in pausing testing or deployments if there is a potential safety hazard, reinforcing our safety-first culture.

Safety assurance routines continuously audit organizational compliance with established safety policies, validating that risk mitigations remain effective over time and feeding operational learnings back into software releases and engineering standards.

By linking frontline reporting, quantitative risk management, and executive board governance, the SMS provides continuous, transparent oversight across the entire lifecycle of Motional's technology and operations.

Field Monitoring and Corrective Actions

Safety management extends continuously into real-world operations through active field monitoring. Motional tracks leading safety metrics and telemetry data across all deployed vehicles to monitor driving behavior, perception performance, actuation smoothness, and hardware health in real time. Evaluating these indicators enables early identification of subtle system anomalies before they manifest as safety-critical events.

When unexpected behavior or field anomalies are detected, Motional initiates structured safety investigations. Dedicated investigation teams analyze sensor logs, software traces, and operational contexts to determine root causes. Findings are used to formulate targeted corrective action plans, which may involve software updates, operational parameter adjustments, or enhanced validation scenarios. Once deployed, the effectiveness of corrective actions is continuously monitored in field telemetry, completing a closed-loop safety improvement cycle.

Regulatory Partnership & Compliance

Operating driverless vehicles on public roads involves comprehensive regulatory accountability and active collaboration with local regulators, transportation authorities, and public safety officials. Motional maintains compliance with applicable federal, state, and local regulatory requirements across operating regions.

At the federal level, Motional adheres to reporting frameworks, including the National Highway Traffic Safety Administration's (NHTSA) Standing General Order regarding automated driving systems. We maintain engagement with regulatory authorities, submitting required event reports and participating in public safety information exchanges.

Direct engagement with law enforcement and emergency first responders is a vital component of public safety readiness. Motional conducts regular training sessions and develops tailored First Responder Interaction Plans for operating locations. These protocols instruct first responders on how to identify robotaxis, interact with onboard safety systems, and communicate directly with Motional operational staff. Our robotaxis are specifically trained to detect emergency vehicle lighting and sirens, initiating appropriate yielding or pullovers to clear emergency corridors and ensure first responders have the right of way.

Pillar Two:
Architect for Resilience

A resilient autonomous system must be designed from the ground up to operate reliably in dynamic environments and tolerate component faults without compromising safety. Pillar Two details the physical hardware architectures, software engineering standards, defense-in-depth cybersecurity protocols, and fault mitigation strategies that ensure Motional AVs maintain safe operation under off-nominal and unexpected conditions.

System Architecture and Design Lifecycle

Motional adopts a rigorous system architecture lifecycle that incorporates structural redundancy, fail-operational design, and deterministic fail-safe responses across hardware and software subsystems. In the event of a critical component malfunction, the system is designed to execute a Minimum Risk Maneuver (MRM), bringing the vehicle safely to a safe state, which may include stopping, pulling over to a shoulder or other safe location, or returning the autonomous vehicle to the depot for maintenance.

Hardware Resilience. Built upon the all-electric Hyundai IONIQ 5 platform, Motional's robotaxi represents a fully integrated Level 4 AV manufactured to automotive-grade standards on a dedicated production assembly line. Vehicle hardware features fully redundant physical systems, including dual-stage power delivery networks, isolated secondary steering actuators, dual-circuit braking architectures, and redundant compute modules. Certified to applicable Federal Motor Vehicle Safety Standards (FMVSS), the vehicle platform ensures structural crashworthiness while providing hardware-level fault tolerance.

Power and compute systems are architected with physical separation and independent circuit protection. Dual high-performance compute nodes continuously cross-monitor system state and sensor data processing. Should a primary compute node experience a hardware interruption, the secondary compute node seamlessly maintains full vehicle motion control and path execution.

Perception hardware incorporates multi-modal sensor redundancy, integrating long and short range LiDARs, long and short range radars, high-resolution optical cameras, acoustic audio sensors, and inertial measurement units (IMUs). Combining complementary sensor modalities provides overlapping 360-degree environmental awareness across diverse lighting, weather, and traffic conditions, compensating for inherent limitations of any individual sensor type.

Software Resilience. Motional's software stack is engineered for fault detection, high availability, and deterministic execution. Key control software modules employ closed-loop feedback verification, constantly comparing targeted trajectory commands with real-world actuator responses.

Motional's autonomy architecture builds redundancy into the AI architecture and provides safety guardrails. Multiple representations of entities in the environment are produced, providing redundant detection of road users around the AV. Also, the system is able to predict multiple potential trajectories for vehicles, cyclists, and pedestrians in the scene, providing multiple possible futures for consideration. The system architecture includes multiple planning approaches and includes a low-latency safety layer planner, providing redundant and timely braking and collision avoidance in the event of a sudden, unexpected safety-critical scenario.

Additionally, an integrated Collision Detection system utilizes multiple sensor inputs, such as accelerometer data and structural telemetry to identify high- and low-impact contact events. Upon detecting impact, the vehicle automatically executes a safe stop and automatically alerts Motional operations specialists, emergency assistance services, and ride hail partners.

Use Case Resilience. To handle passenger and environmental interaction edge cases, robotaxis feature external audio communication systems, automated door and trunk latch controllers, passenger cabin monitoring, and clear visual interface displays. These subsystems allow remote operators or passengers to communicate clearly, resolve unlatched doors automatically before vehicle movement, and ensure cabin security during operations.

Development Lifecycle. Resilience is maintained through a disciplined software release lifecycle. Engineering updates undergo systematic branch isolation, static code analysis, unit testing, and extensive automated regression testing prior to main branch integration. Candidate software releases undergo escalating promotional testing across simulation, hardware-in-the-loop (HIL), closed-course, and supervised public road evaluation before receiving driverless fleet authorization.

Fault Detection and Response

Motional conducts extensive Failure Modes and Effects Analysis (FMEA), Hazard Analysis and Risk Assessment (HARA), and Fault Tree Analysis (FTA) across electronic, mechanical, and software interfaces. Diagnostic health monitors run continuously on onboard systems to detect thermal anomalies, communication latency, voltage fluctuations, or sensor degradation. Detected faults immediately trigger tailored MRMs, ranging from controlled deceleration to nearest shoulder pullovers for minor faults, to, if absolutely necessary, making a rapid, safe stop within the current travel lane when a critical system anomaly occurs. This fail-operational and fail-safe strategy ensures the vehicle can be brought to a controlled stop when necessary

Misuse Identification and Response

Human-system interaction hazards are analyzed to prevent foreseeable vehicle misuse. Onboard cabin sensors and software interlocks detect passenger interference with physical driving controls, seatbelt unbuckling during movement, or premature door opening attempts. When misuse is detected, the system issues immediate visual and audible warnings, prevents vehicle motion, or initiates a controlled pullover to guarantee passenger and public safety.

Cybersecurity Assurance

Motional takes a rigorous, proactive approach to cybersecurity; with forward-looking security engineering practices to defend vehicle control systems, sensor data streams, and fleet communications infrastructure. We have implemented an in-depth cybersecurity framework aligned with international automotive standards, including ISO/SAE 21434, UNECE Regulation 155, and NHTSA cybersecurity recommendations. Security engineering principles are applied across every stage of development, incorporating threat modeling, physical port hardening, secure boot protocols, cryptographic data encryption, and isolated gateway architectures.

Cybersecurity threat analyses evaluate potential attack vectors ranging from localized physical access attempts to wide-area cloud networks. High-assurance cryptographic isolation separates safety-critical vehicle control networks from infotainment and telemetry communications. Motional conducts regular penetration testing in partnership with independent cybersecurity specialists, continuously updating onboard intrusion detection systems (IDS) and over-the-air (OTA) security patches to preserve long-term platform resilience.

Pillar Three:
Drive with Competency

Demonstrating driving competency requires rigorous, empirical verification that the automated driving system plans and executes safe, smooth, and defensive driving actions within its defined operational environment. Pillar Three details the multi-stage Verification and Validation (V&V) methodology, behavioral evaluation frameworks, collision-avoidance capabilities, and emergency response procedures that confirm driving proficiency.

AV Behavioral Competency within Defined ODD

To establish behavioral competency, Motional subjects its driving software to a continuous, multi-stage testing pipeline designed to systematically reduce risk, validate perception and motion planning models, and evaluate full-system performance across increasing levels of operational environment complexity.

Defining the Operational Design Domain (ODD). Behavioral evaluation is anchored strictly within the boundaries of an explicitly defined ODD. For Motional's primary commercial deployment, the ODD encompasses complex urban corridors, multi-lane arterial roadways, regulated intersections, and high-density passenger pickup zones within deployment areas. The ODD specification establishes precise boundaries for operational parameters, including legal speed limits, weather severity thresholds, lighting conditions, roadway geometry, and traffic signal configurations. Motional adheres to AVSC guidelines for ODD definition, employing high-definition 3D mapping and continuous weather monitoring to enforce ODD compliance.

Driving policies. Motional utilizes the AVSC best practice behaviors to define the required competency of the autonomous vehicle. Driving policies are developed for the key behaviors needed within the ODD. We consider infrastructure capabilities (such as intersection handling), responding to other road users (including vulnerable road users, other vehicles), key product capabilities (such as picking up and dropping off passengers), and more. We define a wide variety of scenarios to consider inside each of these capabilities, then define our desired AV behavior in each instance - then test to verify the behavior. These policies ensure the autonomous driving behavior is safe and predictable by other actors on the road, such as drivers, pedestrians, scooters, and cyclists.

Feature V&V. Every proposed software change undergoes extensive targeted and automated evaluation before integration into main development branches. Developers execute unit tests, static code analysis, and large-scale offline simulation runs replaying thousands of real-world road scenarios. Feature testing isolates performance regressions early in code development, verifying algorithmic accuracy across the autonomy sub-modules.

Release V&V. Candidate software releases undergo comprehensive full-stack verification and validation. Large-scale cloud simulation environments are utilized to stress test candidate releases across all safety issues encountered previously on the road and comprehensive exposure to all AVSC behaviors, recreating edge cases, challenging multi-actor interactions, and adverse weather conditions across the entire target ODD. Simulation testing is paired with Hardware in the loop (HIL) testbeds to validate real-time execution timing, bus communication integrity, and fault recovery under physical compute constraints.

Closed-course track testing is utilized to further expose the system to high-severity test scenarios on physical proving grounds using various robotic soft-targets, including vehicles, pedestrians, and cyclists. While these extreme safety critical situations are experienced rarely on public roads, we expose the autonomous vehicle to these challenges repeatedly on the closed-course track to ensure that when a challenging potential collision situation is experienced the Autonomous Driving System is prepared to handle it safely. Standardized international safety protocols, such as Euro NCAP collision avoidance scenarios, are tested on the closed-course track to benchmark performance and ensure readiness.

Following successful simulation and closed-course track validation, supervised public road testing is conducted with trained safety drivers within the target deployment ODD. Safety drivers provide continuous oversight, evaluating real-world driving smoothness, traffic flow integration, and interaction courtesy around pedestrians and surrounding road users.

This multi-stage testing methodology builds a statistically robust body of performance evidence, confirming that candidate software releases demonstrate safe, predictable driving behavior across operational scenarios.

Readiness Decision. The culmination of the V&V lifecycle is a formal driverless readiness analysis. Comprehensive test logs, simulation regression reports, HIL performance data, and risk metrics are compiled into structured readiness dossiers. Motional's Safety Review Board conducts a final audit of this body of evidence, verifying that all safety goals have been satisfied before authorizing driverless software promotion to the operational fleet.

Collision Mitigation

Motional employs a layered collision mitigation strategy engineered to prevent crashes whenever possible and reduce impact severity under unavoidable circumstances. Onboard motion planning algorithms continuously select spatial paths that maximize defensive buffers around surrounding road users. If surrounding actors execute sudden, erratic maneuvers, an onboard low latency planner executes a reflexive response to mitigate a collision and an automatic emergency braking (AEB) and emergency steering sub-routines also deploy immediately to mitigate impact energy.

Incident Response. In the event of an operational incident, Motional maintains a structured Incident Response Program to ensure rapid containment, public safety coordination, and thorough post-event analysis. Onboard sensing is used to automatically detect collision events, bring the vehicle to an immediate stop, activate hazard signaling, and establish direct communication channels between remote operational specialists and ride-hail partners to coordinate with vehicle occupants or emergency services. Comprehensive post-incident investigation protocols analyze event telemetry to inform future safety enhancements across the fleet.

Conclusion

Motional's commitment to safety is built upon the three structural pillars of our Safety Case Framework: Operate with Responsibility, Architect for Resilience, and Drive with Competency. By combining rigorous organizational governance, fault-tolerant hardware and software engineering, and comprehensive verification and validation methodologies, Motional demonstrates that its autonomous vehicles operate with an absence of unreasonable risk. Through transparent methodology and continuous engineering discipline, Motional is helping advance safety standards across the autonomous driving industry while building a safe, reliable, and accessible future for driverless transportation.

