Regulatory and Functional Safety Frameworks

Leo Jaeeun Kim
University of Michigan
General Motors

ABSTRACT

Functional safety and regulatory compliance are critical pillars in the development of collision avoidance systems for autonomous vehicles and advanced driver-assistance systems (ADAS). As these systems assume greater control authority, adherence to structured safety frameworks and validation standards is necessary to ensure reliable and fail-safe operation. This paper reviews and analyzes the key regulatory and functional safety requirements impacting collision avoidance technologies, with a particular focus on ISO 26262, FMVSS 127, and the New Car Assessment Program (NCAP) protocols. ISO 26262 establishes a rigorous lifecycle approach to manage risk arising from hardware and software failures, requiring processes such as Hazard Analysis and Risk Assessment (HARA) and Automotive Safety Integrity Level (ASIL) classification. FMVSS 127 mandates minimum operational capabilities for automatic emergency braking (AEB) systems, while NCAP protocols provide dynamic performance evaluations that influence consumer safety ratings. The paper highlights how early threat prediction methods, such as time-to-collision (TTC) estimation, underpin the technical realization of compliance objectives across these frameworks. A detailed examination of development processes, system validation requirements, and real-world performance standards offers a comprehensive view of the collision avoidance landscape under current regulatory and functional safety expectations.

INTRODUCTION

Ensuring the functional safety of collision avoidance systems is a central requirement for autonomous vehicles and advanced driver-assistance systems (ADAS). As these systems assume greater responsibility for vehicle control, both industry standards and regulatory frameworks impose strict requirements to ensure predictable, reliable, and fail-safe behavior under a wide range of operational conditions. Among these frameworks, ISO 26262 stands as the primary international standard for automotive functional safety, providing structured guidelines for managing risk arising from potential hardware and software failures.

ISO 26262 defines a comprehensive lifecycle for the development of safety-related electrical and electronic systems within road vehicles. It introduces the concept of Automotive Safety Integrity Levels (ASIL), which classify the required rigor of safety measures based on the severity, exposure, and controllability of potential hazardous events. Collision avoidance functionalities, particularly those involving emergency braking, collision warning, and evasive maneuvering, are typically assigned high ASIL ratings (such as ASIL C or D) due to their direct impact on preventing life-threatening scenarios. As such, collision avoidance systems must demonstrate high levels of fault tolerance, systematic integrity, and residual risk reduction through both architectural design and software development processes.

For collision avoidance specifically, ISO 26262 emphasizes the need for early hazard analysis and risk assessment (HARA) to identify hazardous scenarios where loss or degradation of collision prediction could lead to critical outcomes. Safety goals are then derived to ensure timely detection of potential collisions, proper system intervention (e.g., braking or evasive steering), and safe state transitions in the event of system faults. Verification and validation processes under ISO 26262 require comprehensive analysis of both nominal and faulty behavior, including fault injection testing and confirmation of safety mechanisms that ensure degraded system modes still prevent unreasonable risk.

In addition to ISO 26262, collision avoidance performance is subject to consumer evaluation under New Car Assessment Program (NCAP) protocols. NCAP assessments typically evaluate the system's ability to autonomously initiate braking or steering to mitigate frontal collisions, pedestrian impacts, and cyclist crashes, providing safety ratings that influence public perception and commercial success. Furthermore, Federal Motor Vehicle Safety Standards (FMVSS) in the United States establish regulatory requirements for fundamental vehicle safety features, including crashworthiness and minimum braking performance, indirectly impacting the baseline expectations for collision mitigation capabilities.

Together, these standards and regulatory frameworks drive the design, validation, and deployment of collision avoidance systems, ensuring not only technical effectiveness but also systematic compliance with safety-critical operational demands. The predictive time-to-collision estimation approach proposed in this research is developed with these safety objectives in mind, providing a foundational capability to enable timely and reliable collision risk assessment.

ISO 26262

1) Overview of ISO 26262

ISO 26262 is the international standard for functional safety in the automotive industry, providing a structured framework for ensuring that electrical and electronic (E/E) systems in road vehicles operate safely, even in the presence of potential hardware or software faults. It is derived from the broader IEC 61508 functional safety standard but is specifically adapted to the automotive domain, addressing the unique complexity, dynamic behavior, and real-time operational requirements of vehicles.

The ISO 26262 standard defines a comprehensive safety lifecycle encompassing the entire development process, from concept and system design through hardware/software implementation, integration, verification, production, and field operation. It requires safety to be considered from the very earliest stages of development and continuously validated throughout the system's life.

2) Key Concepts in ISO 26262

2.1) Automotive Safety Integrity Level (ASIL)

ASIL is a risk classification scheme that determines the level of safety requirements necessary for a given function. It is calculated based on three factors:

- Severity (S): How severe the harm would be (e.g., injuries, fatalities)
- Exposure (E): How frequently the driving situation occurs
- Controllability (C): How easily the driver or vehicle can avoid the hazardous event

The ASIL levels range from:

- ASIL A (lowest safety integrity) to
- ASIL D (highest, most critical safety integrity)

Collision avoidance functions (like AEB, FCW, evasive steering) typically fall into ASIL C or D, because failure could result in high-severity accidents with limited driver controllability.

2.2) Hazard Analysis and Risk Assessment (HARA)

The HARA process systematically identifies hazardous events that could occur if a system or component fails or behaves incorrectly.
For collision avoidance:

- Hazards include delayed braking, missed collision warnings, or failure to recognize obstacles.
- Each hazard is analyzed to determine the required ASIL level and derived safety goals.

2.3) Safety Goals and Functional Safety Requirements

Once hazards are assessed, safety goals are defined — high-level objectives that must be achieved to mitigate the hazards. These goals are refined into functional safety requirements that drive system, hardware, and software design.

Example for collision avoidance:

- Safety Goal: "The system shall reliably detect and predict imminent collisions under all operational scenarios."
- Functional Requirement: "The system shall estimate time-to-collision with a maximum prediction error of less than X meters/seconds under conditions Y."

2.4) Verification and Validation (V&V)

ISO 26262 requires rigorous V&V processes, including:

- Static analysis (code review, formal proofs)
- Dynamic analysis (testing under fault conditions)
- Fault injection testing (deliberately introducing faults to verify safe behavior)
- ASIL decomposition (splitting safety requirements across redundant paths)

For collision avoidance:

- Testing must demonstrate reliable collision prediction even under degraded sensor inputs or partial system faults.

2.5) Safe State and Fault Tolerance

When faults are detected, the system must transition to a safe state to prevent unreasonable risk.

In collision avoidance:

- Safe state could involve automatically triggering emergency braking.
- Or issuing a fallback maneuver (controlled deceleration) if sensor fusion confidence drops below threshold.

3) ISO 26262 Applied to Collision Avoidance

For collision avoidance systems specifically, ISO 26262 impacts the design as follows:

- Early prediction of collision threats (e.g., using TTC) is a safety goal.
- The system must be able to handle sensor faults, incorrect object detection, or delayed processing.
- Diagnostics must be implemented to monitor sensor health and system status.
- Safe braking or evasive action must occur automatically if risk thresholds are exceeded or fault conditions are detected.

- Verification must include both nominal conditions (normal operation) and fault-injected conditions (sensor dropout, software exception, delayed processing).

Additionally, development under ISO 26262 usually requires:

- Traceability from safety goals → functional requirements → design → implementation → test results
- Development processes following V-model or similar systematic lifecycle models
- Specialized tools and tool qualification if used in safety-critical design (e.g., certified simulators, model checkers)

FMVSS 127

1) Federal Motor Vehicle Safety Standards (FMVSS 127)

The Federal Motor Vehicle Safety Standards (FMVSS) are a set of U.S. regulations established by the National Highway Traffic Safety Administration (NHTSA) to define minimum safety performance requirements for motor vehicles. Among these standards, FMVSS 127 specifically addresses the performance requirements for automatic emergency braking (AEB) systems, reflecting a regulatory push to make active collision mitigation technologies mandatory in light vehicles.

FMVSS 127, formally titled "Automatic Emergency Braking Systems for Light Vehicles," outlines minimum operational capabilities, performance thresholds, and test procedures that AEB systems must meet to comply with federal regulations. Unlike ISO 26262, which focuses on the internal development process and hazard management, FMVSS 127 defines explicit external system performance criteria to ensure that vehicles equipped with AEB can reduce or prevent rear-end collisions under standardized test conditions.

2) Key Requirements of FMVSS 127 for Collision Avoidance

FMVSS 127, formally titled "Automatic Emergency Braking Systems for Light Vehicles," outlines minimum operational capabilities, performance thresholds, and test procedures that AEB systems must meet to comply with federal regulations. Unlike ISO 26262, which focuses on the internal development process and hazard management, FMVSS 127 defines explicit external system performance criteria to ensure that vehicles equipped with AEB can reduce or prevent rear-end collisions under standardized test conditions.

Activation Requirement:

The AEB system must automatically apply braking without driver input when a forward collision is imminent and driver intervention is insufficient.

Performance Testing Scenarios:

Vehicles are evaluated in staged car-to-car rear impact scenarios, including:

- o Approaching a stationary lead vehicle (CCR-S)
- o Approaching a slower-moving lead vehicle (CCR-M)
- o Lead vehicle decelerates sharply (CCR-b braking)

Impact Speed Reduction:

The AEB system must demonstrate a specified minimum reduction in impact speed (e.g., reducing crash severity by defined thresholds depending on scenario setup).

Operational Speed Range:

The system must operate within a specified vehicle speed range, typically between 10 km/h and 100 km/h, depending on the specific sub-test.

False Positive Avoidance:

The AEB system must not trigger unintended braking in scenarios where no legitimate collision threat exists.

Warning Requirements:

A forward collision warning (FCW) signal may be required before AEB activation, depending on system design and compliance pathway.

System Robustness:

The system must function reliably across a variety of conditions, including different lighting environments and lead vehicle characteristics.

NCAP

1) New Car Assessment Program (NCAP)

The New Car Assessment Program (NCAP) is a consumer-focused vehicle safety evaluation initiative operated by various organizations worldwide, such as Euro NCAP, U.S. NCAP, and ASEAN NCAP. NCAPs aim to provide standardized, publicly available vehicle safety ratings that encourage manufacturers to exceed minimum regulatory requirements and offer enhanced safety technologies to consumers. In recent years, NCAP protocols have evolved to include extensive testing of active collision avoidance systems, recognizing their role in preventing accidents before they occur.

Unlike ISO 26262, which governs internal development processes, and FMVSS 127, which establishes minimum legal

compliance for system performance, NCAP focuses on dynamic performance validation under controlled but realistic test conditions. Vehicles are subjected to simulated collision scenarios designed to replicate common real-world crash risks, particularly involving forward collisions and vulnerable road users.

2.1) Active Safety Testing in NCAP

Modern NCAP assessments include comprehensive evaluations of forward collision warning (FCW) and automatic emergency braking (AEB) systems. Key test scenarios for collision avoidance include:

Car-to-Car Rear – Stationary (CCR-S):

Host vehicle approaches a stationary lead vehicle; system must autonomously brake to avoid or mitigate collision.

Car-to-Car Rear – Moving (CCR-M):

Host vehicle approaches a slower-moving lead vehicle.

Car-to-Pedestrian Adult and Child:

Pedestrian crosses into the host vehicle's path; system must detect and brake.

Car-to-Cyclist Nearside:

Cyclist crosses vehicle path laterally from near side.

AEB Junction Assist (Euro NCAP specific):

Host vehicle must avoid or mitigate collisions during turning maneuvers into crossing traffic.

Each scenario has defined testing speeds, detection distances, and performance thresholds that the vehicle's collision avoidance system must meet or exceed to achieve full NCAP points.

2.2) Scoring and Evaluation Criteria

NCAP protocols evaluate several dimensions of active safety performance:

- Detection and Threat Assessment Timing:
  Early detection and timely collision threat recognition are critical. Late detection results in lower scores or failed test cases.
- Braking Response Time and Deceleration:
  AEB must autonomously initiate braking within prescribed time windows and decelerate the vehicle sufficiently to avoid or mitigate the collision.
- Warning Effectiveness (for FCW Systems):
  Systems that issue earlier and appropriate driver warnings are scored more favorably.
- Impact Speed Reduction:
  Even if a collision cannot be fully avoided, reducing the impact speed below defined thresholds earns partial credit.
- Robustness Across Conditions:
  Systems are tested under varying conditions such as daylight, night time with low lighting, and different pedestrian/cyclist profiles.

CONCLUSION

The integration of functional safety principles and regulatory compliance is essential for the reliable deployment of collision avoidance systems in modern autonomous vehicles and advanced driver-assistance systems. Through detailed analysis of ISO 26262, FMVSS 127, and NCAP protocols, this research illustrates how safety engineering, risk management, and system performance validation converge to form a comprehensive safety framework for collision avoidance functionality.

ISO 26262 establishes structured development and verification processes, emphasizing hazard analysis, ASIL-driven design rigor, and systematic validation under both nominal and faulty conditions. FMVSS 127 imposes mandatory minimum performance requirements for automatic emergency braking systems, ensuring that collision avoidance technologies achieve tangible reductions in crash severity under standardized testing conditions. Meanwhile, NCAP protocols drive system innovation and refinement through competitive, consumer-visible active safety testing.

Predictive methodologies such as time-to-collision estimation play a foundational role in enabling systems to meet these requirements, supporting early intervention and enhancing robustness against dynamic threats. As the automotive industry advances toward higher levels of automation and increased system complexity, a disciplined approach to functional safety, regulatory compliance, and predictive risk estimation will remain fundamental to achieving safe and reliable collision avoidance capabilities.

Future work may extend this analysis to include emerging standards for cybersecurity (ISO 21434), safety of intended functionality (ISO/PAS 21448, SOTIF), and new international regulations governing autonomous vehicle operation (such as UNECE WP.29 frameworks), offering a broader perspective on the evolving landscape of safety assurance in intelligent mobility systems.

REFERENCES

[1] International Organization for Standardization, *ISO 26262: Road vehicles – Functional safety*, Parts 1–10, 2nd ed., Geneva, Switzerland, Dec. 2018.

[2] U.S. Department of Transportation, National Highway Traffic Safety Administration (NHTSA), *Federal Motor Vehicle Safety Standards; Automatic Emergency Braking Systems for Light Vehicles, FMVSS No. 127*, Notice of Proposed Rulemaking, Docket No. NHTSA-2023-0009, May 2023. [Online]. Available: https://www.nhtsa.gov/laws-regulations/fmvss-127-automatic-emergency-braking-systems-light-vehicles

[3] Euro NCAP, *Assessment Protocol – Vulnerable Road User Protection (VRU) Version 11.0*, Euro NCAP, Feb. 2023. [Online]. Available: https://www.euroncap.com/en/for-engineers/protocols/vru/

[4] Euro NCAP, *Assessment Protocol – Safety Assist (Version 10.0)*, Euro NCAP, Feb. 2023. [Online]. Available: https://www.euroncap.com/en/for-engineers/protocols/safety-assist/

[5] U.S. New Car Assessment Program (NCAP), *Request for Comments – New Car Assessment Program (NCAP) Improvements*, NHTSA, Docket No. NHTSA-2022-0002, Mar. 2022. [Online]. Available: https://www.nhtsa.gov/laws-regulations/new-car-assessment-program-ncap

[6] ISO/PAS 21448:2019, *Road vehicles – Safety of the Intended Functionality (SOTIF)*, International Organization for Standardization, Geneva, Switzerland, 2019.