International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

SOTIF (ISO 21448) for Heavy-Duty Commercial Vehicle ADAS: A Practical Implementation Framework

Mahesh Kumar Shanmugam

Submitted:01/11/2023 **Revised:** 08/12/2023 **Accepted:** 22/12/2023

Abstract: ISO 21448, formally addressing the Safety of the Intended Functionality (SOTIF), was published in 2022 to address safety risks arising from functional insufficiencies in advanced driver assistance systems and automated driving functions, even when no system malfunction has occurred [1]. This distinguishes SOTIF from ISO 26262, which primarily addresses hazards caused by electrical and electronic system faults [2]. As of 2023, practical SOTIF implementation guidance for heavy-duty commercial vehicle Advanced Driver Assistance Systems (ADAS) remained limited in public literature. The only publicly available heavy-truck SOTIF example was a concept-level platooning hazard analysis, not a production-oriented methodology for Class 8 ADAS features [5]. This paper proposes a six-phase SOTIF implementation framework for Class 8 commercial vehicle ADAS, covering item definition, hazard identification, triggering-condition analysis, functional modification, verification and validation evidence generation, and release-operation feedback. The framework addresses truck-specific SOTIF challenges including variable payload, trailer articulation, pneumatic brake response, sensor mounting height, maintenance variability, and commercial duty cycles. The proposed approach provides original practical guidance for applying SOTIF to production-relevant heavy-duty ADAS features such as Adaptive Cruise Control, Automatic Emergency Braking Systems, Lane Departure Warning, and Traffic Sign Recognition. The contribution of this paper is a truck-specific, implementation-oriented SOTIF framework that bridges the gap between ISO 21448 process principles and the operational realities of Class 8 commercial vehicle safety engineering.

Keywords: *SOTIF, ISO 21448, ISO 26262, Class 8 trucks, heavy-duty vehicles, ADAS, AEBS, ACC, LDW, TSR, triggering conditions, commercial vehicle safety*

1. Introduction

Sensor-based Advanced Driver Assistance Systems are increasingly deployed in heavy-duty commercial vehicles. Functions such as Adaptive Cruise Control (ACC), Automatic Emergency Braking Systems (AEBS), Lane Departure Warning (LDW), and Traffic Sign Recognition (TSR) are intended to reduce collision risk, improve driver support, and enhance fleet safety performance. However, the safe deployment of these systems requires more than traditional fault-based safety engineering. A system may be electrically healthy, software may execute correctly, and diagnostics may show no malfunction, yet the ADAS function may still behave unsafely because its perception capability, functional specification, or assumptions about the driving environment are insufficient.

Kettering University, USA
Email Id : email2maheshs@gmail.com

ISO 26262 asks whether the electrical or electronic system behaves safely when faults occur. SOTIF asks a different question: can the system create unreasonable risk while operating exactly as designed because its intended functionality is incomplete or its performance is insufficient for the real-world scenario encountered [1], [2]. For example, a radar may be functioning correctly and the perception software may execute without error, yet the system may fail to classify a partially occluded vehicle, a motorcycle cut-in, or a stationary object under a bridge shadow. Such a case is not necessarily a hardware or software malfunction. It is a SOTIF problem.

In 2023, SOTIF was still an emerging engineering discipline, especially in commercial vehicle organizations. ISO 21448 was understood mainly by functional safety specialists, ADAS and automated-driving safety teams, and selected Tier 1

suppliers. It was not yet broadly institutionalized across commercial vehicle original equipment manufacturers. The ASAM 2022 Test Specification Study Group report described ISO 21448 as generating significant industry interest, while also emphasizing that implementation requires concrete test strategies, scenario-based validation, and process alignment [3]. TÜV SÜD's 2023 SOTIF white paper similarly framed SOTIF as a risk-based approach requiring practical verification and validation strategies for estimating residual risk in ADAS and automated driving systems [4].

For heavy-duty commercial vehicles, the implementation gap was even more pronounced. Public SOTIF guidance was largely developed around passenger-car ADAS and automated driving contexts. Heavy-duty trucks introduce additional complexity because vehicle behavior depends on payload, trailer configuration, air-brake dynamics, pneumatic delay, tractor-trailer interaction, sensor mounting height, road-spray exposure, and fleet maintenance practices. The 2021 NHTSA/Battelle heavy-truck platooning hazard analysis remains one of the closest public examples of applying SOTIF thinking to commercial trucks, but it was concept-level and constrained by limited functional specification detail [5].

This paper addresses that gap by proposing a practical six-phase SOTIF implementation framework for Class 8 commercial vehicle ADAS. The framework is designed for production-oriented engineering use and covers item definition, hazard identification, triggering-condition analysis, functional modification, verification and validation evidence, and release-operation feedback. The paper focuses on ACC, AEBS, LDW, and TSR because these functions combine perception, decision logic, human-machine interaction, and vehicle actuation in ways that create meaningful SOTIF exposure for heavy-duty trucks.

2. Background: ISO 21448 and the Meaning of SOTIF

ISO 21448 defines SOTIF as the absence of unreasonable risk caused by hazards resulting from functional insufficiencies in the intended functionality or performance insufficiencies in the implementation of the intended functionality [1]. In practical terms, SOTIF is concerned with hazards that arise even when the system has not failed in the ISO 26262 sense. This distinction is essential for sensor-based ADAS because camera, radar, lidar, map, and perception algorithms can behave within specification while still failing to interpret a difficult scene correctly.

Table 1. Comparison Between ISO 26262 and ISO 21448

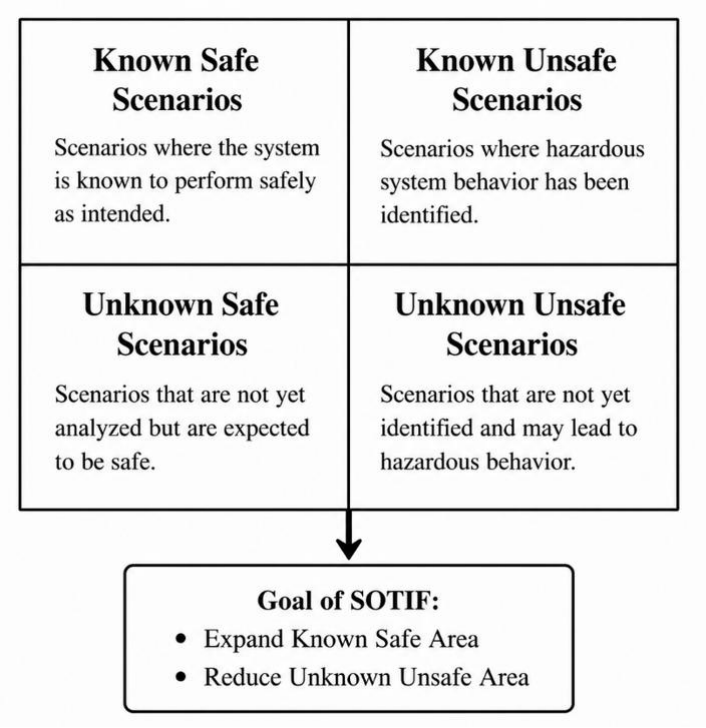
Aspect	ISO 26262	ISO 21448 (SOTIF)
Primary Focus	Fault-based safety	Functional insufficiency safety
Trigger	Hardware/software malfunction	Correct operation with unsafe outcome
Main Concern	Random/systematic failures	Perception and specification limitations
Example	Radar power failure	Radar misclassifies object
Safety Goal	Fault tolerance	Scenario robustness
Key Output	ASIL safety requirements	Triggering-condition mitigation

ISO 26262 addresses functional safety of electrical and electronic systems. It focuses on random hardware failures, systematic software faults, diagnostic coverage, safety mechanisms, Automotive Safety Integrity Levels, and fault-handling behavior [2]. SOTIF excludes those fault-based concerns. Instead, it addresses scenarios in which the system is operating normally but its functionality or assumptions are insufficient. For ADAS, these insufficiencies often involve perception limits, environmental ambiguity, unusual object presentation, driver misuse, or

operating conditions outside the validated Operational Design Domain.

ISO 21448 is particularly relevant to functions where proper situational awareness is safety-critical and depends on complex sensors and algorithms. These include emergency intervention systems, lane support functions, driver assistance technologies, and driving automation functions. The standard is therefore directly relevant to ACC, AEBS, LDW, and TSR in Class 8 trucks.

Figure 1. Four SOTIF Scenario Areas



SOTIF commonly organizes the scenario space into four conceptual areas. The first area consists of known safe scenarios, where the system performs as intended. The second area consists of known unsafe scenarios, where hazardous behavior has been identified. The third area consists of unknown unsafe scenarios, where hazardous behavior may exist but has not yet been discovered. The fourth area consists of unknown safe scenarios, where the system would behave safely but the case has not yet been characterized. The SOTIF process aims to enlarge the known safe area, eliminate or mitigate known unsafe scenarios, and reduce the unknown unsafe area through systematic discovery.

Scenario-based testing has therefore become central to SOTIF implementation. ISO 34502 provides terminology and guidance for test scenarios in automated driving systems and supports the broader move toward structured scenario-based validation [13]. SAE J3016 also provides automation terminology that helps clarify driver role, automation level, and system responsibility in ADAS and automated driving discussions [14]. For heavy-duty vehicles, however, scenario definitions must include truck-specific variables such as trailer type, load state, braking architecture, sensor mounting height, and commercial operating environment.

3. Related Work

General SOTIF literature had expanded by 2023, but implementation practice remained developing. The ASAM 2022 Test Specification Study Group report connected SOTIF with scenario-based testing and noted that SOTIF does not provide detailed instructions for how virtual testing, proving-ground testing, and real driving should be combined [3]. This is important because SOTIF evidence cannot realistically be generated by one testing method alone. It requires a multi-pillar validation approach.

Burton et al. discussed ISO 21448 in relation to uncertainty, functional insufficiencies, triggering

conditions, acceptance criteria, and unknown unsafe scenarios [6]. Their work emphasized that safety assurance for systems using machine learning and complex perception is difficult because uncertainty cannot be completely eliminated. Birkemeyer, King, and Schaefer reviewed scenario-generation techniques for SOTIF-compliant testing and concluded that scenario generation remained an essential missing detail in practical SOTIF implementation [7]. A later 2023 study on SOTIF-compliant scenario generation proposed semi-concrete scenarios and parameter sampling as a way to systematically explore relevant scenario spaces [8].

Putze et al. examined quantification for SOTIF validation and highlighted uncertainty around quantitative acceptance criteria and risk decomposition [9]. Their work is particularly relevant because commercial vehicle manufacturers must eventually justify whether residual SOTIF risk is acceptable for a specific Operational Design Domain. Adee et al. studied environmental perception limitations in automated driving, reinforcing the importance of modeling perception insufficiencies rather than treating them as ordinary software defects [10]. Koné et al. proposed a method to guide the search for hazardous scenarios in autonomous vehicle safety validation, supporting the broader need for structured triggering-condition discovery [11].

For commercial vehicles specifically, public literature was much thinner. The NHTSA/Battelle heavy-truck platooning hazard analysis applied SOTIF thinking to two representative truck platooning concepts and identified difficult hazards including unexpected traffic stoppage, road debris, tire-wear differences, motorcycle cut-ins, evasive steering, and driver inattentiveness [5]. However, the authors also noted that limited functional specification detail made SOTIF analysis challenging. Therefore, the report is best understood as evidence of the gap rather than a complete implementation framework.

Heavy-vehicle regulatory activity also increased by 2023. The NHTSA/FMCSA NPRM on Heavy Vehicle Automatic Emergency Braking proposed performance tests for stopped lead vehicle, slower-moving lead vehicle, decelerating lead vehicle, and false-activation scenarios [12]. Although this proposed rule was not a SOTIF standard, it highlighted the growing importance of heavy-vehicle perception and braking reliability in safety-critical ADAS.

The related work therefore confirms a clear gap. By 2023, there was no public, Class 8 commercial vehicle-specific SOTIF framework covering production ADAS features such as ACC, AEBS, LDW, and TSR. This paper responds directly to that gap.

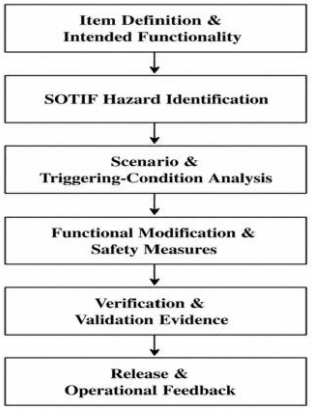
4. SOTIF Process Framework for Class 8 ADAS

This section presents the core contribution of the paper: a six-phase SOTIF implementation framework designed specifically for Class 8 commercial vehicle ADAS.

4.1 Phase 1: Item Definition and Intended Functionality

The SOTIF process must begin with a precise item definition. For a Class 8 truck ADAS program, the item definition should identify the ADAS feature or integrated feature package, the sensors used, the actuators commanded, the driver role assumed, the Operational Design Domain, and the vehicle configurations included in the release scope.

Figure 2. Six-Phase SOTIF Implementation Framework for Class 8 ADAS



For example, an AEBS item definition should specify whether the system uses radar only, camera-radar fusion, map support, or additional object classification logic. It should also define whether the ADAS function has authority over service-brake commands, whether it can request engine torque reduction, and whether it interacts with electronic stability control, retarder control, engine braking, trailer braking, or regenerative braking.

Class 8 trucks require more detailed item definitions than passenger vehicles because vehicle response depends on configuration. A system validated on a 6x4 diesel tractor with a dry van trailer may not behave identically on a battery electric tractor, tanker trailer, or heavily loaded refrigerated combination. Therefore, the item definition must state which wheelbases, axle layouts, trailer types, load states, brake configurations, powertrains, and sensor packages are in scope.

The item definition must also specify driver responsibility. For Level 1 or Level 2 ADAS, the driver remains responsible for supervision and control. However, SOTIF analysis must still examine foreseeable misuse, over-trust, nuisance-alert fatigue, and misunderstanding of system boundaries.

4.2 Phase 2: SOTIF Hazard Identification and Risk Evaluation

SOTIF hazard identification differs from ISO 26262 hazard analysis. ISO 26262 asks what happens when a system element fails. SOTIF asks what becomes hazardous even when the system works according to its specification [1], [2].

Truck ADAS examples include a camera correctly producing low-confidence lane detection in snow, a radar correctly tracking the wrong object near a curve, TSR correctly reading a speed sign intended for an adjacent lane, or AEBS failing to classify a stopped vehicle because its appearance lies outside the validated training domain. These are not malfunctions. They are functional or performance insufficiencies.

For each identified hazard, engineers should describe the functional insufficiency, the triggering condition, the hazardous vehicle or driver behavior, and the potential consequence. Severity, exposure, and controllability may be assessed using a framework similar to ISO 26262 HARA, but the causal mechanism is different. The focus is not component failure; it is performance limitation under normal operation.

In Class 8 vehicles, controllability must be interpreted carefully. A professional driver may be trained, but the vehicle has longer stopping distances, greater mass, trailer articulation, and larger blind zones. A false braking event, missed braking event, or nuisance warning may have consequences that differ substantially from a passenger car.

4.3 Phase 3: Scenario and Triggering-Condition Analysis

The third phase classifies relevant scenarios into the four SOTIF areas: known safe, known unsafe, unknown unsafe, and unknown safe. Known unsafe scenarios can be identified through Operational Design Domain analysis, feature specification review, vehicle configuration assessment, fleet use-case analysis, prior test failures, crash data, warranty data, driver complaints, and expert workshops.

Unknown unsafe scenarios require active discovery. Relevant techniques include broad scenario generation, simulation sweeps, parameter sampling, naturalistic driving data analysis, fleet shadow-mode testing, anomaly detection, targeted proving-ground testing, and post-release monitoring [7], [8], [11]. The objective is not to prove that unknown unsafe scenarios no longer exist. That is unrealistic. The objective is to provide a reasoned argument that discovery effort has reduced the likelihood of hazardous unknown scenarios to an acceptable level for the intended Operational Design Domain.

For truck ADAS, triggering-condition analysis must include variables frequently absent from passenger-car validation: trailer type, trailer angle, gross combination weight, brake temperature, pneumatic delay, sensor contamination, sensor mounting height, fleet maintenance variability, road spray, and professional driver interaction patterns.

4.4 Phase 4: Functional Modification and Safety Measures

When known unsafe scenarios are identified, the system must be modified or restricted. The modification may involve changes to the Operational Design Domain, sensor fusion strategy, warning timing, braking thresholds, lane model,

TSR logic, human-machine interface, driver monitoring assumptions, maintenance instructions, fallback behavior, or release scope.

For heavy-duty trucks, functional modification may include load-aware braking calibration, sensor-cleanliness diagnostics, trailer-compatibility restrictions, speed-range limitations, driver warnings when environmental conditions exceed validated boundaries, and stricter ODD exits in construction zones or poor visibility.

Functional modification should be traceable. Each known unsafe scenario should be linked to a specific mitigation, and each mitigation should be verified through appropriate evidence. This prevents the SOTIF process from becoming a checklist exercise.

4.5 Phase 5: Verification and Validation Evidence Generation

SOTIF evidence generation should combine multiple validation methods. Known unsafe scenarios should be verified through targeted tests. Unknown unsafe scenarios should be explored through simulation, proving-ground tests, fleet shadow testing, data mining, and post-release monitoring [3], [4], [9].

Table 2. SOTIF Validation Activities for Heavy-Truck ADAS

Validation Activity	Purpose
Simulation	Broad scenario exploration
SIL/HIL Testing	Logic and integration verification
Proving-Ground Testing	Controlled hazardous scenarios
Fleet Shadow Testing	Unknown scenario discovery
Post-Release Monitoring	Continuous SOTIF improvement

For Class 8 ADAS, validation evidence should include perception-performance tests under environmental variation, scenario-based simulation with triggering-condition injection, software-in-the-loop testing, hardware-in-the-loop testing, model-in-the-loop testing, proving-ground tests with soft targets, fleet shadow-mode data, data mining for false positives and false negatives, driver misuse evaluation, ODD boundary testing, HMI comprehension testing, and field monitoring.

Validation should also consider communication and actuation pathways. Heavy trucks rely on vehicle networks, air-brake timing, electronic stability control interaction, and trailer brake behavior. Therefore, SOTIF evidence should not be limited to sensor perception; it should include the complete chain from perception to decision, warning, driver response, braking command, and vehicle response.

4.6 Phase 6: Release and Operation

SOTIF should not end at release. It should remain a living engineering process. Every field event, near miss, nuisance activation, missed detection, driver complaint, maintenance issue, or warranty claim should feed back into the scenario catalog and safety case.

A Class 8 truck may operate for years across changing routes, trailers, payloads, weather conditions, and maintenance states. This makes post-release monitoring especially important. The released system should include mechanisms for logging relevant events, detecting scenario drift, reviewing fleet data, updating triggering-condition catalogs, and revising ODD limitations when necessary.

5. Sensor Performance Limitations in Heavy-Truck ADAS

Heavy-truck ADAS sensor limitations arise from both general perception challenges and truck-specific packaging conditions.

5.1 Camera Limitations

Camera-based ADAS functions may be affected by glare from low or setting sun, reduced nighttime visibility, dirty windshields, rain-induced contrast

loss, snow and fog, road spray from preceding vehicles, worn lane markings, non-standard construction markings, unusual traffic signs, partial object occlusion, and bright reflections from wet road surfaces.

For LDW and TSR, camera performance is especially important. Worn lane markings may reduce lane-model confidence. Temporary work-zone signs may conflict with map data. A sign intended for a nearby exit ramp may be incorrectly interpreted as applying to the truck's lane. These are typical SOTIF issues because the camera and software may be operating as designed while still producing unsafe or misleading output.

5.2 Radar Limitations

Radar limitations include multipath reflections from metallic roadside structures and bridges, ambiguity in classifying stationary objects at highway speeds, limited angular resolution for closely spaced targets, mechanical misalignment after vibration or maintenance, and confusion between relevant and irrelevant targets near curves, ramps, and interchanges.

AEBS and ACC depend heavily on radar object tracking. In heavy trucks, radar installation height and bumper geometry may differ significantly from passenger cars. Therefore, detection angles, target selection, and clutter rejection must be evaluated specifically for truck geometry.

5.3 Truck Packaging Limitations

Truck packaging introduces distinctive SOTIF limitations. Sensors are often mounted higher than on passenger cars, creating different field-of-view geometry and blind zones. Sensors are exposed to stronger vibration, road salt, insects, ice, mud, diesel exhaust residue, and commercial-duty contamination.

Maintenance activities also create risk. Windshield replacement, bumper repair, bracket servicing, or sensor cover replacement may alter calibration. In fleet environments, inconsistent maintenance quality can become a triggering condition. Tractor-trailer combination geometry also creates rear and side occlusion patterns that are not present in passenger vehicles.

5.4 Infrastructure Limitations

Infrastructure limitations include worn or missing lane markings, temporary construction lane delineators, arrow boards, steel plates, bridge structures, overpasses, tunnel entries and exits, curves, road grades, ramps, narrow lanes, and non-standard roadway geometry.

These conditions can cause a correctly functioning perception system to produce uncertain or incorrect outputs. For SOTIF, such conditions must be modeled as triggering conditions rather than treated only as test failures.

6. Triggering-Condition Analysis

Truck-specific triggering conditions can be organized into environmental, infrastructure, traffic, vehicle-specific, and human-use categories.

6.1 Environmental Triggering Conditions

Environmental triggering conditions include rain, fog, snow, low sun, nighttime operation, road spray, dust, sensor icing, mud, and sensor surface contamination. These conditions degrade perception performance and may cause lane, object, or sign recognition uncertainty.

Table 3. Truck-Specific Triggering Conditions for ADAS

Category	Triggering Condition	Potential SOTIF Impact
Environmental	Fog, snow, glare	Reduced perception accuracy
Infrastructure	Construction zones	Incorrect lane interpretation
Traffic	Motorcycle cut-ins	Delayed classification
Truck-Specific	Trailer articulation	Occlusion and braking variability
Human Use	Driver over-trust	Delayed intervention

6.2 Infrastructure Triggering Conditions

Infrastructure triggering conditions include worn lane markings, temporary construction lanes, work-zone lane shifts, steel plates, bridge structures, tunnel entries and exits, road shadows, curves, grades, ramps, narrow lanes, and non-standard road geometry. These conditions may cause correct software to make incorrect assumptions about lane boundaries, object relevance, or applicable speed limits.

6.3 Traffic Triggering Conditions

Traffic triggering conditions include stopped traffic queues, slow-moving lead vehicles, hard-braking lead vehicles, cut-in maneuvers, motorcycles, vulnerable road users near the lane, emergency vehicles, debris, and vehicles partially outside the ego lane.

The NHTSA/Battelle platooning report identified similar truck-relevant hazards, including unexpected traffic stoppage, road debris, motorcycle cut-ins, evasive steering, tire-wear differences, and driver inattentiveness [5]. This confirms that truck-specific triggering conditions are not hypothetical.

6.4 Truck-Specific Triggering Conditions

Truck-specific triggering conditions include load state, trailer type, trailer brake condition, tire wear, brake temperature, pneumatic delay, sensor mounting height, tractor-cab geometry, and maintenance state variability. These factors directly influence vehicle response and sensor interpretation.

6.5 Human-Use Triggering Conditions

Human-use triggering conditions include driver over-trust, reduced attention when ADAS is active, nuisance-alert fatigue, misuse outside the intended ODD, failure to clean sensors, failure to verify alignment after maintenance, and misunderstanding of system limitations during handover.

SOTIF must address foreseeable human interaction because the driver remains part of the safety concept for most Class 8 ADAS features.

7. ISO 26262 and SOTIF Integration

ISO 26262 and ISO 21448 divide the safety problem rather than duplicate it. ISO 26262 is activated when the system malfunctions because of hardware failure, software error, diagnostic fault, or systematic development error [2]. SOTIF is activated when the system works correctly but the intended functionality or implementation performance is insufficient for the real-world scenario [1].

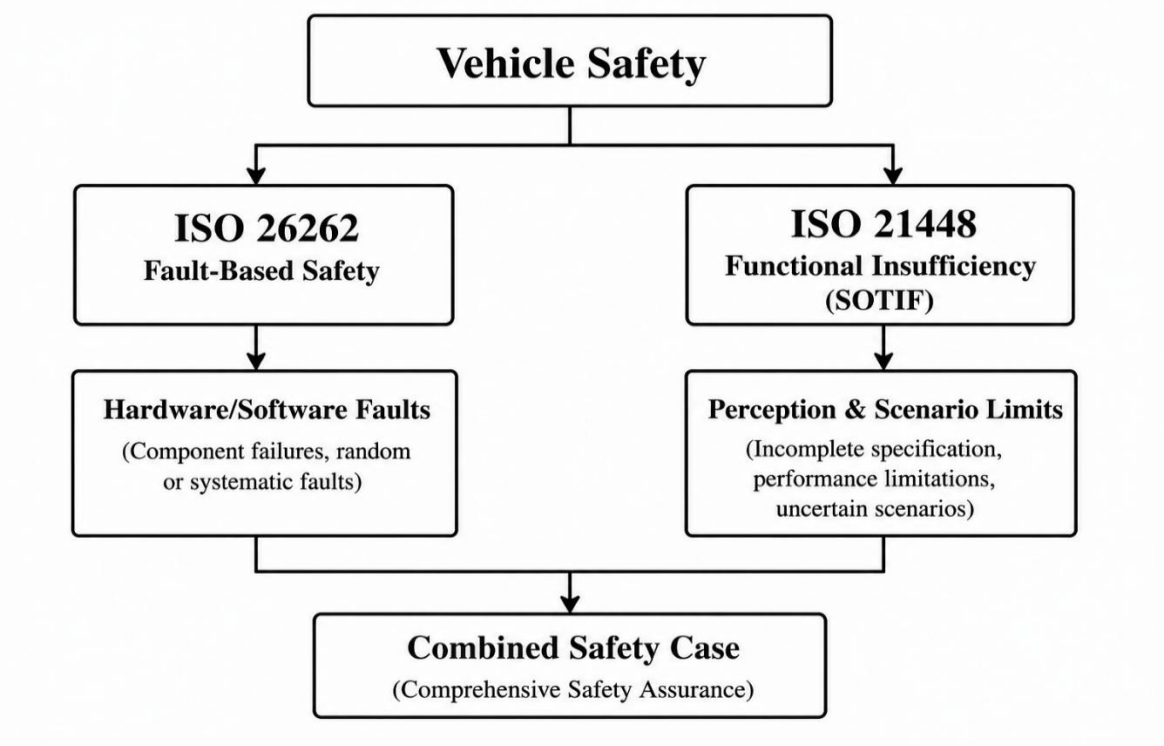


Figure 3. Integrated ISO 26262 + SOTIF Safety Relationship

In a combined implementation, both processes should share the same item definition, Operational Design Domain definition, interface descriptions, driver-role assumptions, and safety case structure. The ISO 26262 process produces functional safety goals, ASIL classifications, safety mechanisms, diagnostics, fault-handling behavior, and hardware/software safety requirements. The SOTIF process produces performance limitations, triggering conditions, scenario coverage requirements, ODD restrictions, HMI requirements, and SOTIF validation targets.

TÜV SÜD's 2023 SOTIF white paper described SOTIF and functional safety as complementary aspects of system safety and emphasized that both perspectives are required for ADAS and automated driving functions [4]. The ASAM 2022 report similarly described ISO 21448 as a necessary extension to ISO 26262 for ADAS and automated driving because complex sensor-software interaction cannot be treated like traditional deterministic vehicle functions [3].

For Class 8 trucks, integration is especially important. A missed AEBS detection may be a SOTIF issue if caused by perception insufficiency, but it may be an ISO 26262 issue if caused by radar power failure or brake-control communication loss. Both processes must feed the same safety case.

8. Acceptance Criteria for Commercial Vehicle SOTIF

In 2023, the most defensible position was that SOTIF acceptance criteria must be explicitly defined by the OEM for each safety goal and Operational Design Domain. ISO 21448 provides process logic, but practitioners must still define what acceptable residual risk means for their system, market, fleet use case, and safety argument [1].

Burton et al. emphasized that SOTIF requires acceptance criteria for safety goals and that such criteria may be refined and allocated to subsystems such as perception or decision functions [6]. Putze et al. further argued that rigorous quantitative SOTIF validation requires consistent terminology and risk decomposition when acceptance criteria are used [9].

For a Class 8 truck ADAS program, practical acceptance criteria should include evidence that all identified known unsafe scenarios have been eliminated, mitigated, or restricted by ODD controls. Feature performance must meet defined thresholds for detection, warning timing, braking response, lane-warning behavior, and sign recognition. False-positive and false-negative rates must remain within justified limits.

Acceptance criteria should also require that sensor degradation and ODD exits are detected and communicated to the driver. Driver misuse cases should be addressed through HMI design, warnings, training, or ODD restrictions. Unknown unsafe scenario discovery should be supported through simulation, proving-ground testing, fleet shadow data, and post-release monitoring.

The objective is not to prove that unknown unsafe scenarios no longer exist. Rather, the objective is to demonstrate that sufficient discovery effort has been undertaken and that residual risk is justified for the intended ODD.

9. Practical Implementation Recommendations

Commercial vehicle OEMs implementing SOTIF for the first time should treat it as a safety engineering process, not a compliance paperwork exercise. The first implementation should begin with one safety-critical feature such as AEBS or ACC. Engineers should define the item and ODD carefully, identify truck-specific assumptions, build a triggering-condition catalog, and connect every SOTIF hazard to verification or validation evidence.

Second, SOTIF must be built around real commercial vehicle use. The process should include trailer combinations, load states, brake behavior, tire wear, sensor maintenance variability, professional driver behavior, and actual operating environments such as highways, freight terminals, loading docks, construction zones, rural roads, and weigh stations.

Third, acceptance criteria should be defined before release testing begins. Teams should define safety goals, scenario-coverage targets, performance thresholds, false-positive limits, false-negative limits, ODD exit behavior, driver notification rules, and field-monitoring triggers early in development.

The NHTSA/Battelle platooning analysis demonstrates that even a concept-level SOTIF application requires functional specifications,

operational scenarios, driver behavior assumptions, and iteration when unsafe scenarios are identified [5]. Production programs require even stronger discipline.

10. Conclusion

This paper proposed a practical six-phase SOTIF implementation framework for Class 8 commercial vehicle ADAS. The framework covers item definition, SOTIF hazard identification, scenario and triggering-condition analysis, functional modification, verification and validation evidence generation, and release-operation feedback.

The paper argued that heavy-duty commercial vehicles require dedicated SOTIF treatment because their safety performance depends on factors that are less prominent in passenger vehicles, including payload variation, trailer interaction, air-brake dynamics, sensor packaging, maintenance variability, and commercial duty cycles.

The original contribution of this paper is a Class 8-specific SOTIF implementation framework for production-relevant ADAS features such as ACC, AEBS, LDW, and TSR. The framework translates ISO 21448 principles into practical engineering activities suitable for commercial vehicle OEMs and suppliers.

SOTIF should be treated as living documentation. Every field event, near miss, nuisance activation, missed detection, or driver complaint should update the scenario catalog and safety case. As commercial vehicle ADAS deployment expands, practical SOTIF implementation will become increasingly important for ensuring that safety-critical systems remain robust not only against faults, but also against functional insufficiencies in the real world.

References

[1] International Organization for Standardization. (2022). *ISO 21448: Road vehicles—Safety of the intended functionality*. ISO.

[2] International Organization for Standardization. (2018). *ISO 26262: Road vehicles—Functional safety*. ISO.

[3] Burton, S., Gauerhof, L., & Heinzemann, C. (2012). Making the case for safety of machine learning in highly automated driving. *Lecture Notes in Computer Science*, 7613, 5–16.

[4] Burton, S., Herd, B., Lünstedt, S., & Schaefer, I. (2023). Addressing uncertainty in the safety assurance of machine-learning. *Frontiers in Computer Science*, 5, 1–16.

[5] Birkemeyer, L., King, C., & Schaefer, I. (2023). Is scenario generation ready for SOTIF? A systematic literature review. *arXiv Preprint*, arXiv:2308.02273.

[6] Koné, A., Espié, S., & Gruyer, D. (2023). An approach to guide the search for potentially hazardous scenarios for autonomous vehicle safety validation. *Applied Sciences*, 13(11), 6717.

[7] Putze, L., Westhofen, L., Koopmann, T., Böde, E., & Neurohr, C. (2023). On quantification for SOTIF validation of automated driving systems. *arXiv Preprint*, arXiv:2304.10170.

[8] Ulbrich, S., Menzel, T., Reschka, A., Schuldt, F., & Maurer, M. (2015). Defining and substantiating the terms scene, situation, and scenario for automated driving. In *2015 IEEE 18th International Conference on Intelligent Transportation Systems* (pp. 982–988). IEEE.

[9] Bagschik, G., Menzel, T., & Maurer, M. (2018). Ontology based scene creation for the development of automated vehicles. In *2018 IEEE Intelligent Vehicles Symposium* (pp. 1813–1820). IEEE.

[10] Riedmaier, S., Ponn, T., Ludwig, D., Schick, B., & Diermeyer, F. (2020). Survey on scenario-based safety assessment of automated vehicles. *IEEE Access*, 8, 87456–87477.

[11] Koopman, P., & Wagner, M. (2017). Autonomous vehicle safety: An interdisciplinary challenge. *IEEE Intelligent Transportation Systems Magazine*, 9(1), 90–96.

[12] Kalra, N., & Paddock, S. M. (2016). *Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability?* RAND Corporation.

[13] SAE International. (2021). *SAE J3016: Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles*. SAE International.

[14] International Organization for Standardization. (2022). *ISO 34502: Road vehicles—Scenario-based safety evaluation framework*. ISO.

[15] National Highway Traffic Safety Administration & Battelle Memorial Institute. (2021). *Hazard analysis of concept heavy-truck platooning systems*. U.S. Department of Transportation.

[16] National Highway Traffic Safety Administration & Federal Motor Carrier Safety Administration. (2023). *Heavy vehicle automatic emergency braking; AEB test devices: Notice of proposed rulemaking*. *Federal Register*, 88(128).

[17] United Nations Economic Commission for Europe. (2013). *UN Regulation No. 131: Advanced Emergency Braking Systems (AEBS)*.

[18] United Nations Economic Commission for Europe. (2013). *UN Regulation No. 130: Lane Departure Warning Systems (LDWS)*.

[19] U.S. Code of Federal Regulations. (2023). *Federal Motor Vehicle Safety Standard No. 121: Air brake systems* (49 CFR §571.121).

[20] U.S. Code of Federal Regulations. (2023). *Federal Motor Vehicle Safety Standard No. 136: Electronic stability control systems for heavy vehicles* (49 CFR §571.136).

[21] PEGASUS Project Consortium. (2019). *PEGASUS method: An overview of the PEGASUS project results*. German Aerospace Center (DLR).

[22] Adee, R., et al. (2023). Systematic modeling approach for environmental perception limitations in automated driving. *arXiv Preprint*, arXiv:2303.04029.

[23] ASAM e.V. (2022). *ASAM test specification study group report 2022*. ASAM.

[24] TÜV SÜD. (2023). *Safety in ADAS/AD—SOTIF: A risk-based approach*. TÜV SÜD White Paper.