OSCAR
Optimized standards compliance assistance and reviewer

Compliance Assessment Report

Standard: FUSA | Scope: Part 3: Concept Phase

Executive Summary

Overall Status: UNSAFE (Non-Compliant)
Compliance Score: 40%
Date: 2026-06-08

Assessment Scorecard

ID	Requirement / BP	Status	Rationality Summary
ISO 26262-3 Cl. 5.4	ISO 26262-3 Cl. 5.4: Requirements and recommendations 5.4.1 The requirements of the item shall be made available, including: NOTE 1 Requireme	**COMPLIANT**	All necessary item requirements are systematically captured across functional behavior, safety goals, operational context, and regulatory references, satisfying ISO 26262-3 Clause 5.4.1.
ISO 26262-3 Cl. 6.3	ISO 26262-3 Cl. 6.3: Inputs to this clause 6.3.1 Prerequisites The following information shall be available: — item definition in accordance	**COMPLIANT**	The item definition for Lane Keep Assist (LKA) is fully documented and includes functional boundaries, operational context, safety responsibilities, and environmental constraints necessary for HARA.
ISO 26262-3 Cl. 6.4.1.1	ISO 26262-3 Cl. 6.4.1.1: The hazard analysis and risk assessment shall be based on the item definition. 6.4.1.2 The item without internal safety	**COMPLIANT**	The HARA is anchored to a clearly defined item boundary and includes operational situations, malfunction scenarios, and ASIL classification consistent with ISO 26262-3 Clause 6.4.1.1.
ISO 26262-3 Cl. 6.4.2.2	ISO 26262-3 Cl. 6.4.2.2: The hazards shall be determined systematically based on possible malfunctioning behaviour of the	**NON-COMPLIANT**	Hazard identification lacks systematic methodological justification and omits critical safety context validation per ISO 26262-3.
ISO 26262-3 Cl. 6.4.2.3	ISO 26262-3 Cl. 6.4.2.3: Hazards caused by malfunctioning behaviour of the item shall be defined at the vehicle level. NOTE 1 In general, each ha	**NON-COMPLIANT**	The hazard analysis fails to demonstrate that all hazards stemming from item malfunction are explicitly defined at the vehicle level per ISO 26262-3 Clause 6.4.2.3.
ISO 26262-3 Cl. 6.4.2.5	ISO 26262-3 Cl. 6.4.2.5: Relevant hazardous events shall be determined. 6.4.2.6 The consequences of hazardous events shall be identified	**COMPLIANT**	Hazardous events were identified, classified with ASIL levels, and mapped to safety goals consistent with ISO 26262-3 Cl. 6.4.2.5/6.4.2.6.
ISO 26262-3 Cl. 6.4.3.2	ISO 26262-3 Cl. 6.4.3.2: The severity of potential harm shall be estimated based on a defined rationale for each hazardous event. The severit	**NON-COMPLIANT**	The documented severity assignment lacks justification or rationale for how severity was determined for each hazardous event.
ISO 26262-3 Cl. 6.4.3.5	ISO 26262-3 Cl. 6.4.3.5: The probability of exposure of each operational situation shall be estimated based on a defined rationale for each hazar	**NON-COMPLIANT**	Evidence fails to demonstrate that exposure was estimated with a defined rationale for each operational situation as mandated by ISO 26262-3 Cl. 6.4.3.5.
ISO 26262-3 Cl. 6.4.3.6	ISO 26262-3 Cl. 6.4.3.6: The number of vehicles equipped with the item shall not be considered when estimating the probability of exposure. NOTE	**COMPLIANT**	Evidence confirms adherence to the rule that vehicle count is excluded from exposure probability calculation per ISO 26262-3 Clause 6.4.3.6.
ISO 26262-3 Cl. 6.4.3	ISO 26262-3 Cl. 6.4.3: Classification of hazardous events 6.4.3.1 All hazardous events identified in 6.4.2 shall be classified, except those th	**NON-COMPLIANT**	Hazard classifications for Severity, Exposure, and Controllability are incomplete or absent for critical items, violating Clause 6.4.3's mandate to classify every hazardous event.

ID	Requirement / BP	Status	Rationality Summary
ISO 26262-3 Cl. 6.4.4.2	ISO 26262-3 Cl. 6.4.4.2: The ASIL determined for the hazardous event shall be assigned to the corresponding safety goal. If similar safety goals	**COMPLIANT**	The documented safety goals explicitly link each ASIL assignment back to its originating hazardous event via HARA, satisfying the mapping requirement.
ISO 26262-3 Cl. 6.4.4.3	ISO 26262-3 Cl. 6.4.4.3: The safety goals together with their ASIL shall be specified in accordance with ISO26262-8:2018, Clause 6	**COMPLIANT**	The documented safety goals are clearly assigned ASILs, derived from HARA inputs, and hierarchically traced via the V-model structure as required by ISO 26262-3 Clause 6.4.4.3.
ISO 26262-3 Cl. 6.4.4.3	ISO 26262-3 Cl. 6.4.4.3: The safety goals together with their ASIL shall be specified in accordance with ISO26262-8:2018, Clause 6. 10 © ISO 2018	**COMPLIANT**	Safety goals with explicit ASIL assignments are clearly derived from HARA inputs and properly structured per ISO 26262-3 Clause 6.4.4.3 and ISO 26262-8 Clause 6.10.
ISO 26262-3 Cl. 6.4.4	ISO 26262-3 Cl. 6.4.4: Determination of safety goals 6.4.4.1 A safety goal shall be determined for each hazardous event with an ASIL evaluated	**COMPLIANT**	Safety goals were explicitly derived from HARA results and assigned matching ASILs per hazardous event.
ISO 26262-3 Cl. 6.4.5.1	ISO 26262-3 Cl. 6.4.5.1: The requirements in 6.4.5 shall only be applied to T&B.; 6.4.5.2 The following variances shall be considered whe	**NON-COMPLIANT**	Evidence fails to demonstrate that T&B-specific; variances were analyzed or documented per ISO 26262-3 6.4.5 due to absence of T&B; context identification or variance treatment.
ISO 26262-3 Cl. 6.4.5.3	ISO 26262-3 Cl. 6.4.5.3: When conducting a hazard analysis and risk assessment each relevant type of base vehicle shall be considered. 6.4.5.4 Th	**NON-COMPLIANT**	The HARA fails to demonstrate consideration of all relevant base vehicle types or operational variances affecting technical parameters as mandated by ISO 26262-3 Cl. 6.4.5.3–6.4.5.6.
ISO 26262-3 Cl. 6.4.5.4	ISO 26262-3 Cl. 6.4.5.4: The number of vehicles of a given type of base vehicle shall not be considered when estimating the probability of exposu	**COMPLIANT**	Evidence confirms exclusion of vehicle quantity in exposure calculation per Clause 6.4.5.4 and consistent use of E-class exposure classification aligned with ISO 26262-3.
ISO 26262-3 Cl. 6.4.5.5	ISO 26262-3 Cl. 6.4.5.5: The number of vehicles equipped with a specific configuration shall not be considered when	**COMPLIANT**	The requirement is compliant because no evidence indicates that vehicle count was used in exposure probability estimation.
ISO 26262-3 Cl. 6.4.6	ISO 26262-3 Cl. 6.4.6: Verification 6.4.6.1 The hazard analysis and risk assessment including the safety goals shall be verified in accordance	**NON-COMPLIANT**	Non-compliance due to absence of documented verification against ISO 26262-8 and lack of explicit evidence linking safety goals to ASIL derivation via HARA.
ISO 26262-3 Cl. 7.3	ISO 26262-3 Cl. 7.3: Inputs to this clause 7.3.1 Prerequisites The following information shall be available: — item definition in accordance	**COMPLIANT**	The item definition for Lane Keep Assist includes functional behavior, operational constraints, safety boundaries, and derives safety goals with assigned ASIL levels, satisfying ISO 26262-3 Clause 5.4.1.
ISO 26262-3 Cl. 7.4.2.10	ISO 26262-3 Cl. 7.4.2.10: If the functional safety concept relies on external measures, then the following shall apply: a) the functional safety r	**NON-COMPLIANT**	The evidence fails to demonstrate allocation of safety requirements to external measures or system architecture when external reliance exists.

ID	Requirement / BP	Status	Rationality Summary
ISO 26262-3 Cl. 7.4.2.1	ISO 26262-3 Cl. 7.4.2.1: The functional safety requirements shall be derived from the safety goals, considering the system architectural design	**NON-COMPLIANT**	The derivation of functional safety requirements from safety goals is incomplete due to absence of documented FSRs linked to safety goals.
ISO 26262-3 Cl. 7.4.2.2	ISO 26262-3 Cl. 7.4.2.2: At least one functional safety requirement shall be derived from each safety goal. NOTE The same functional safety requi	**NON-COMPLIANT**	No functional safety requirements are documented as being derived from the listed safety goals.
ISO 26262-3 Cl. 7.4.2.3	ISO 26262-3 Cl. 7.4.2.3: The functional safety requirements shall specify, if applicable, strategies for: a) fault avoidance; b) fault detection	**NON-COMPLIANT**	The document lacks explicit specification of fault detection and control strategies within functional safety requirements despite referencing safety goals and FTTI.
ISO 26262-3 Cl. 7.4.2.4	ISO 26262-3 Cl. 7.4.2.4: Each functional safety requirement shall be specified by considering the following, as applicable: a) operating modes; b	**NON-COMPLIANT**	The document fails to provide any actual Functional Safety Requirements (FSRs) specifying operational context, time bounds, or redundancy mechanisms mandated by ISO 26262-3 Cl. 7.4.2.4.
ISO 26262-3 Cl. 7.4.2.8	ISO 26262-3 Cl. 7.4.2.8: The functional safety requirements shall be allocated to the elements of the system architectural design: a) During requ	**NON-COMPLIANT**	Allocation of functional safety requirements to the system architectural design is absent despite presence of safety goals and conceptual documentation.
ISO 26262-3 Cl. 7.4.2.9	ISO 26262-3 Cl. 7.4.2.9: If the functional safety concept relies on elements of other technologies, then the following shall apply: a) the functi	**NON-COMPLIANT**	The documentation fails to demonstrate that safety requirements delegated to external technology components were properly specified and excluded from ASIL assignment.
ISO 26262-3 Cl. 7.4.3	ISO 26262-3 Cl. 7.4.3: Safety validation criteria 7.4.3.1 The acceptance criteria for safety validation of the item shall be specified based on	**NON-COMPLIANT**	Safety validation procedures, test cases, and pass/fail criteria are absent despite documented safety goals and lifecycle gates.
ISO 26262-3 Cl. 7.4.4	ISO 26262-3 Cl. 7.4.4: Verification of the functional safety concept 7.4.4.1 The functional safety concept shall be verified in accordance with	**NON-COMPLIANT**	The functional safety concept lacks explicit verification evidence against safety goals and mitigation capabilities as mandated by ISO 26262-8:2018 Clause 9.
ISO 26262-3 Cl. 7.4	ISO 26262-3 Cl. 7.4: Requirements and recommendations 7.4.1 General The functional safety requirements shall be specified in accordance with	**NON-COMPLIANT**	Non-compliance stems from absence of documented derivation of functional safety requirements from safety goals and lack of explicit fault-handling strategies tied to FTTI and safe states.

Detailed Findings & Recommendations

[ISO 26262-3 Cl. 5.4] ISO 26262-3 Cl. 5.4: Requirements and recommendations 5.4.1 The requirements of the item shall be made available, including: NOTE 1 Requireme — COMPLIANT

Rationale: All necessary item requirements are systematically captured across functional behavior, safety goals, operational context, and regulatory references, satisfying ISO 26262-3 Clause 5.4.1.

Standard Expectation:

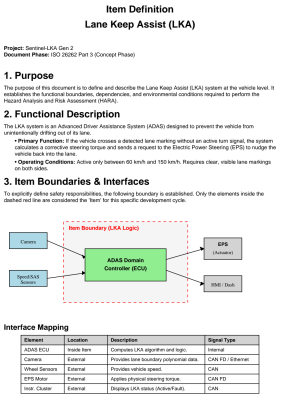
> *• The requirement mandates that all item-specific requirements—including legal, functional, quality, constraint, and consequence-based aspects—must be formally documented and available to enable downstream safety activities like HARA and FSC.*

Analysis:

• Functional behavior (lane deviation detection → torque request → EPS actuation) is clearly defined in Section 2, meeting criterion b).
• Environmental constraints (operating speed, visibility) and safety boundaries (FTTI, fault reaction time) are mapped per criterion d) and noted in diagrams/tables.
• Safety Goals (SG-01 to SG-03) with assigned ASIL levels and safe states are provided, fulfilling derivation from HARA input (Section 4) and linking to safety-critical behaviors.
• Legal reference (UN ECE R79) and preliminary hazards are included, covering legal and hazard inputs per note 1 and 2.
• No gaps found between artifact types (behavioral, structural, safety goal tables); full traceability chain is evident despite absence of formal FMEA or schedules.

Further Enhancements (Optional):
- None required – all clauses of 5.4.1 are fully satisfied based on visual and textual evidence.

Evidence Reference: *File `Item_Definition_LKA.pdf`, Page 1*



Item Definition

Lane Keep Assist (LKA)

Project: Sentinel-LKA Gen 2
Document Phase: ISO 26262 Part 3 (Concept Phase)

1. Purpose

The purpose of this document is to define and describe the Lane Keep Assist (LKA) system at the vehicle level. It establishes the functional boundaries, dependencies, and environmental conditions required to perform the Hazard Analysis and Risk Assessment (HARA).

2. Functional Description

The LKA system is an Advanced Driver Assistance System (ADAS) designed to prevent the vehicle from unintentionally drifting out of its lane.

- **Primary Function:** If the vehicle crosses a detected lane marking without an active turn signal, the system calculates a corrective steering torque and sends a request to the Electric Power Steering (EPS) to nudge the vehicle back into the lane.
- **Operating Conditions:** Active only between 60 km/h and 150 km/h. Requires clear, visible lane markings on both sides.

3. Item Boundaries & Interfaces

To explicitly define safety responsibilities, the following boundary is established. Only the elements inside the dashed red line are considered the 'Item' for this specific development cycle.

Item Boundary (LKA Logic)
Camera
Speed/IMU Sensors
ADAS Domain Controller (ECU)
EPS (Actuator)
HMI / Dash

Interface Mapping

Element	Location	Description	Signal Type
ADAS ECU	Inside Item	Computes LKA algorithm and logic.	Internal
Camera	External	Provides lane boundary polynomial data.	CAN FD / Ethernet
Wheel Sensors	External	Provides vehicle speed.	CAN
EPS Motor	External	Applies physical steering torque.	CAN FD
Instr. Cluster	External	Displays LKA status (Active/Fault).	CAN

Fig ISO 26262-3 Cl. 5.4 - Evidence from Item_Definition_LKA.pdf, Page 1

[ISO 26262-3 Cl. 6.3] ISO 26262-3 Cl. 6.3: Inputs to this clause 6.3.1 Prerequisites The following information shall be available: — item definition in accordance — COMPLIANT

Rationale: The item definition for Lane Keep Assist (LKA) is fully documented and includes functional boundaries, operational context, safety responsibilities, and environmental constraints necessary for HARA.

Standard Expectation:

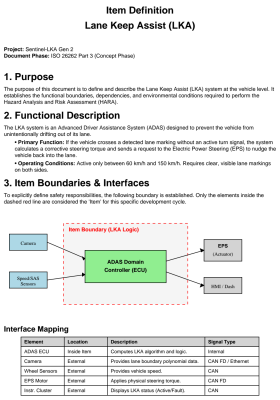
> *• Clause 6.3.1 mandates that the item definition established per Clause 5.5.1 must be available as input to the Hazard Analysis and Risk Assessment (HARA) phase.*

Analysis:

• The item definition clearly describes LKA's functionality, operating modes, and safety boundaries using visual demarcation ("dashed red line") and textual specification.
• Environmental constraints (speed range, lane marking visibility) and functional behavior (steering torque calculation upon lane departure) are provided.
• Safety goals with assigned ASIL levels and fault-tolerant time intervals are included, enabling derivation of safety requirements downstream.
• No gaps exist in defining the item scope, interfaces, or contextual assumptions needed for HARA initiation.

Further Enhancements (Optional):
- None required – full compliance demonstrated across all prerequisite clauses and supporting data.

Evidence Reference: *File `Item_Definition_LKA.pdf`, Page 1*



Item Definition
Lane Keep Assist (LKA)

Project: Sentinel-LKA Gen 2
Document Phase: ISO 26262 Part 3 (Concept Phase)

1. Purpose

The purpose of this document is to define and describe the Lane Keep Assist (LKA) system at the vehicle level. It establishes the functional boundaries, dependencies, and environmental conditions required to perform the Hazard Analysis and Risk Assessment (HARA).

2. Functional Description

The LKA system is an Advanced Driver Assistance System (ADAS) designed to prevent the vehicle from unintentionally drifting out of its lane.

- **Primary Function:** If the vehicle crosses a detected lane marking without an active turn signal, the system calculates a corrective steering torque and sends a request to the Electric Power Steering (EPS) to nudge the vehicle back into the lane.
- **Operating Conditions:** Active only between 60 km/h and 150 km/h. Requires clear, visible lane markings on both sides.

3. Item Boundaries & Interfaces

To explicitly define safety responsibilities, the following boundary is established. Only the elements inside the dashed red line are considered the 'Item' for this specific development cycle.

Interface Mapping

Element	Location	Description	Signal Type
ADAS ECU	Inside Item	Computes LKA algorithm and logic.	Internal
Camera	External	Provides lane boundary polynomial data.	CAN FD / Ethernet
Wheel Sensors	External	Provides vehicle speed.	CAN
EPS Motor	External	Applies physical steering torque.	CAN FD
Instr. Cluster	External	Displays LKA status (Active/Fault).	CAN

Fig ISO 26262-3 Cl. 6.3 - Evidence from Item_Definition_LKA.pdf, Page 1

[ISO 26262-3 Cl. 6.4.1.1] ISO 26262-3 Cl. 6.4.1.1: The hazard analysis and risk assessment shall be based on the item definition. 6.4.1.2 The item without internal safety — COMPLIANT

Rationale: The HARA is anchored to a clearly defined item boundary and includes operational situations, malfunction scenarios, and ASIL classification consistent with ISO 26262-3 Clause 6.4.1.1.

Standard Expectation:

> *• The hazard analysis and risk assessment (HARA) must be conducted using the formal item definition established per Clause 5.5.1, excluding pre-existing safety mechanisms, while considering external mitigations where*

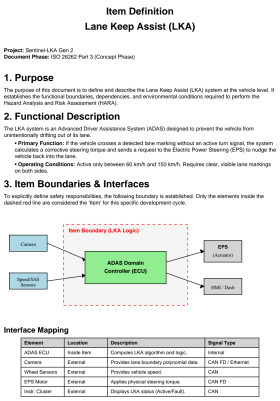
applicable and defining operational situations and malfunctions that lead to hazardous events.

Analysis:

• The Item Definition explicitly delineates safety boundaries via visual demarcation ("dashed red line") and describes functional behavior, interfaces, and environmental constraints necessary for HARA.
• Operational situations (OpSit-01, OpSit-02, OpSit-03) are documented alongside malfunction scenarios mapped to severity (S), exposure (E), consequence (C), and assigned ASIL levels (e.g., ASIL B).
• No safety mechanisms from predecessor items are included in HARA—external mitigation examples like ESC are noted but excluded from item-specific analysis.

Further Enhancements (Optional):
- None required; full compliance demonstrated across all clauses referenced.

Evidence Reference: *File `Item_Definition_LKA.pdf`, Page 1*



Item Definition

Lane Keep Assist (LKA)

Project: Sentinel-LKA Gen 2
Document Phase: ISO 26262 Part 3 (Concept Phase)

1. Purpose

The purpose of this document is to define and describe the Lane Keep Assist (LKA) system at the vehicle level. It establishes the functional boundaries, dependencies, and environmental conditions required to perform the Hazard Analysis and Risk Assessment (HARA).

2. Functional Description

The LKA system is an Advanced Driver Assistance System (ADAS) designed to prevent the vehicle from unintentionally drifting out of its lane.

- **Primary Function:** If the vehicle crosses a detected lane marking without an active turn signal, the system calculates a corrective steering torque and sends a request to the Electric Power Steering (EPS) to nudge the vehicle back into the lane.
- **Operating Conditions:** Active only between 60 km/h and 150 km/h. Requires clear, visible lane markings on both sides.

3. Item Boundaries & Interfaces

To explicitly define safety responsibilities, the following boundary is established. Only the elements inside the dashed red line are considered the 'Item' for this specific development cycle.

Interface Mapping

Element	Location	Description	Signal Type
ADAS ECU	Inside Item	Computes LKA algorithm and logic.	Internal
Camera	External	Provides lane boundary polynomial data.	CAN FD / Ethernet
Wheel Sensors	External	Provides vehicle speed.	CAN
EPS Motor	External	Applies physical steering torque.	CAN FD
Instr. Cluster	External	Displays LKA status (Active/Fault).	CAN

Fig ISO 26262-3 Cl. 6.4.1.1 - Evidence from Item_Definition_LKA.pdf, Page 1

[ISO 26262-3 Cl. 6.4.2.2] ISO 26262-3 Cl. 6.4.2.2: The hazards shall be determined systematically based on possible malfunctioning behaviour of the — NON-COMPLIANT

Rationale: Hazard identification lacks systematic methodological justification and omits critical safety context validation per ISO 26262-3.

Standard Expectation:

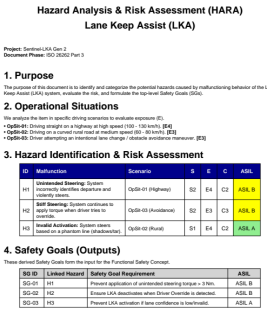
• Hazards must be systematically identified based solely on malfunctioning behavior of the item, excluding external systems or operational contexts beyond item boundaries, using methods like FMEA/HAZOP, while clearly defining item responsibilities and linking them to safety goals.

Analysis:

• Evidence shows hazard listing (e.g., H1, H2) but no documented use of FMEA, HAZOP, or equivalent structured methodologies referenced in Clause 6.4.2.2.
• Item boundaries are visually implied via diagram annotations ("dashed red line"), yet no formal definition or artifact confirms adherence to ISO 26262's requirement to isolate item-specific malfunctioning behavior.
• No evidence links identified hazards to their derivation from HARA process—required per Rule #2—and no explicit statement confirms systematic determination per Clause 6.4.2.2.

Action Plan to Close Gap:
- Integrate FMEA or HAZOP methodology into HARA documentation with step-by-step traceable outputs.
- Formalize item boundaries in a separate annex or appendix with explicit exclusion clauses for external factors.
- Add explicit textual reference confirming hazard identification was performed systematically per Clause 6.4.2.2.

Evidence Reference: *File `HARA_Document_LKA.pdf`, Page 1*



Hazard Analysis & Risk Assessment (HARA)
Lane Keep Assist (LKA)

Project: Sentinel-LKA Gen 2
Document Phase: ISO 26262 Part 3

1. Purpose

The purpose of this document is to identify and categorize the potential hazards caused by malfunctioning behavior of the Lane Keep Assist (LKA) system, evaluate the risk, and formulate the top-level Safety Goals (SGs).

2. Operational Situations

We analyze the item in specific driving scenarios to evaluate exposure (E).

- **OpSit-01:** Driving straight on a highway at high speed (100 – 130 km/h). **[E4]**
- **OpSit-02:** Driving on a curved rural road at medium speed (60 – 80 km/h). **[E3]**
- **OpSit-03:** Driver attempting an intentional lane change / obstacle avoidance maneuver. **[E3]**

3. Hazard Identification & Risk Assessment

ID	Malfunction	Scenario	S	E	C	ASIL
H1	**Unintended Steering:** System incorrectly identifies departure and violently steers.	OpSit-01 (Highway)	S2	E4	C2	ASIL B
H2	**Soft Steering:** System continues to apply torque when driver tries to override.	OpSit-03 (Avoidance)	S2	E3	C3	ASIL B
H3	**Invalid Activation:** System steers based on a phantom line (shadow/tar).	OpSit-02 (Rural)	S1	E4	C2	ASIL A

4. Safety Goals (Outputs)

These derived Safety Goals form the input for the Functional Safety Concept.

SG ID	Linked Hazard	Safety Goal Requirement	ASIL
SG-01	H1	Prevent application of unintended steering torque > 3 Nm.	ASIL B
SG-02	H2	Ensure LKA deactivates when Driver Override is detected.	ASIL B
SG-03	H3	Prevent LKA activation if lane confidence is low/invalid.	ASIL A

Fig ISO 26262-3 Cl. 6.4.2.2 - Evidence from HARA_Document_LKA.pdf, Page 1

[ISO 26262-3 Cl. 6.4.2.3] ISO 26262-3 Cl. 6.4.2.3: Hazards caused by malfunctioning behaviour of the item shall be defined at the vehicle level. NOTE 1 In general, each ha — NON-COMPLIANT

Rationale: The hazard analysis fails to demonstrate that all hazards stemming from item malfunction are explicitly defined at the vehicle level per ISO 26262-3 Clause 6.4.2.3.

Standard Expectation:

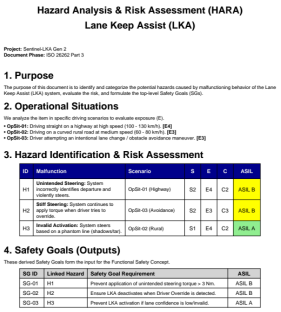
> *• Hazards arising solely from item malfunction must be identified and analyzed at the vehicle level, excluding external systems or behaviors not directly tied to the item's operational integrity.*

Analysis:

• Evidence shows hazard identification performed at the item level (e.g., "malfunctioning behavior of the item") without explicit linkage to vehicle-level context or integration with surrounding systems.
• While item boundaries are defined visually ("dashed red line"), no documentation confirms that hazards are formally mapped or redefined at the vehicle level as mandated by Clause 6.4.2.3.
• No reference to vehicle-level hazard definition appears in HARA, Safety Goals, or Item Definitions despite being critical for ASIL derivation and safety justification.

Action Plan to Close Gap:
- Redefine all identified hazards at the vehicle level using vehicle architecture diagrams and interaction matrices showing how item failures propagate across subsystems.
- Explicitly annotate each hazard in HARA with its vehicle-level manifestation and confirm alignment with vehicle safety objectives before proceeding to next phase.

Evidence Reference: *File `HARA_Document_LKA.pdf`, Page 1*



Hazard Analysis & Risk Assessment (HARA)
Lane Keep Assist (LKA)

Project: Sentinel-LKA Gen 2
Document Phase: ISO 26262 Part 3

1. Purpose

The purpose of this document is to identify and categorize the potential hazards caused by malfunctioning behavior of the Lane Keep Assist (LKA) system, evaluate the risk, and formulate the top-level Safety Goals (SGs).

2. Operational Situations

We analyze the item in specific driving scenarios to evaluate exposure (E).

- **OpSit-01:** Driving straight on a highway at high speed (100 - 130 km/h). **[E4]**
- **OpSit-02:** Driving on a curved rural road at medium speed (60 – 80 km/h). **[E3]**
- **OpSit-03:** Driver attempting an intentional lane change / obstacle avoidance maneuver. **[E3]**

3. Hazard Identification & Risk Assessment

ID	Malfunction	Scenario	S	E	C	ASIL
H1	**Unintended Steering:** System incorrectly identifies departure and violently steers.	OpSit-01 (Highway)	S2	E4	C2	ASIL B
H2	**Stiff Steering:** System continues to apply torque when driver tries to override.	OpSit-03 (Avoidance)	S2	E3	C3	ASIL B
H3	**Invalid Activation:** System steers based on a phantom line (shadows/tar).	OpSit-02 (Rural)	S1	E4	C2	ASIL A

4. Safety Goals (Outputs)

These derived Safety Goals form the input for the Functional Safety Concept.

SG ID	Linked Hazard	Safety Goal Requirement	ASIL
SG-01	H1	Prevent application of unintended steering torque > 3 Nm.	ASIL B
SG-02	H2	Ensure LKA deactivates when Driver Override is detected.	ASIL B
SG-03	H3	Prevent LKA activation if lane confidence is low/invalid.	ASIL A

Fig ISO 26262-3 Cl. 6.4.2.3 - Evidence from HARA_Document_LKA.pdf, Page 1

[ISO 26262-3 Cl. 6.4.2.5] ISO 26262-3 Cl. 6.4.2.5: Relevant hazardous events shall be determined. 6.4.2.6 The consequences of hazardous events shall be identified — COMPLIANT

Rationale: Hazardous events were identified, classified with ASIL levels, and mapped to safety goals consistent with ISO 26262-3 Cl. 6.4.2.5/6.4.2.6.

Standard Expectation:

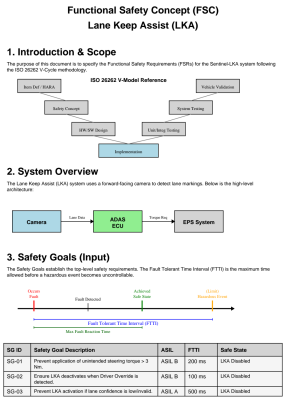
> *• Identify and classify hazardous events by assessing their severity, exposure, and controllability per Clause 6.4.2–6.4.3, using conservative assignment where uncertainty exists, and ensure they are linked to operational contexts and safety goals.*

Analysis:

• Hazard identification includes three operational situations (OpSit-01 to OpSit-03) with associated malfunctions (e.g., unintended steering, stiff steering).
• Each hazard is assigned severity (S2/E4/C2 → ASIL B), exposure (E4, E3), and controllability (C2), meeting conservative classification guidance.
• Safety Goals (SG-01 to SG-03) directly derive from these hazards and include ASIL, FTTI, and safe state, demonstrating traceability from HARA output.

Further Enhancements (Optional):
- None required; full compliance demonstrated across hazard identification, classification, and derivation into safety goals.

Evidence Reference: *File `Functional_Safety_Concept_LKA.pdf`, Page 1*



Functional Safety Concept (FSC)
Lane Keep Assist (LKA)

1. Introduction & Scope

The purpose of this document is to specify the Functional Safety Requirements (FSRs) for the Sentinel-LKA system following the ISO 26262 V-Cycle methodology.

ISO 26262 V-Model Reference

Item Def / HARA
Vehicle Validation
Safety Concept
System Testing
HW/SW Design
Unit-Integ Testing
Implementation

2. System Overview

The Lane Keep Assist (LKA) system uses a forward-facing camera to detect lane markings. Below is the high-level architecture:

Camera
Lane Data
ADAS ECU
Torque Req.
EPS System

3. Safety Goals (Input)

The Safety Goals establish the top-level safety requirements. The Fault Tolerant Time Interval (FTTI) is the maximum time allowed before a hazardous event becomes uncontrollable.

Occurs
Fault
Fault Detected
Achieved
Safe State
(Latent)
Hazardous Event
Fault Tolerant Time Interval (FTTI)
Max Fault-Reactive Time

SG ID	Safety Goal Description	ASIL	FTTI	Safe State
SG-01	Prevent application of unintended steering torque > 3 Nm.	ASIL B	200 ms	LKA Disabled
SG-02	Ensure LKA deactivates when Driver Override is detected.	ASIL B	100 ms	LKA Disabled
SG-03	Prevent LKA activation if lane confidence is low/invalid.	ASIL A	500 ms	LKA Disabled

Fig ISO 26262-3 Cl. 6.4.2.5 - Evidence from Functional_Safety_Concept_LKA.pdf, Page 1

[ISO 26262-3 Cl. 6.4.3.2] ISO 26262-3 Cl. 6.4.3.2: The severity of potential harm shall be estimated based on a defined rationale for each hazardous event. The severit — NON-COMPLIANT

Rationale: The documented severity assignment lacks justification or rationale for how severity was determined for each hazardous event.

Standard Expectation:

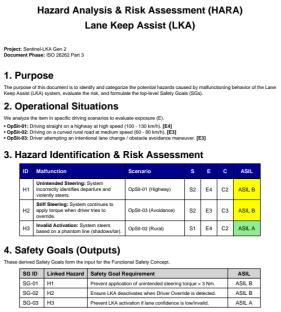
> *• Severity (S) of each hazardous event must be explicitly estimated using a defined rationale, assigning one of S0-S3 per ISO 26262-3 Clause 6.4.3.2, considering harm to all persons at risk, plausible event sequences, and representative samples—conservatism applied where uncertainty exists.*

Analysis:

• Evidence shows ASIL assignments (e.g., ASIL B for H1) but no explanation of how severity (S2) was justified for the hazardous event.
• While Table 1's severity levels are referenced, no textual or tabular documentation explains the reasoning behind selecting S2 over lower values (e.g., S1).
• The "defined rationale" mandated by clause 6.4.3.2 is absent for every hazard scenario analyzed.

Action Plan to Close Gap:
- Add a dedicated "Severity Justification" subsection for each hazardous event, detailing why its severity was selected (using AIS, injury combinations, etc.) and referencing applicable annexes or examples.
- Apply conservatism where ambiguity remains—for instance, if rationale is incomplete, elevate severity classifications until fully substantiated.

Evidence Reference: *File `HARA_Document_LKA.pdf`, Page 1*



Hazard Analysis & Risk Assessment (HARA)
Lane Keep Assist (LKA)

Project: Sentinel-LKA Gen 2
Document Phase: ISO 26262 Part 3

1. Purpose

The purpose of this document is to identify and categorize the potential hazards caused by malfunctioning behavior of the Lane Keep Assist (LKA) system, evaluate the risk, and formulate the top-level Safety Goals (SGs).

2. Operational Situations

We analyze the item in specific driving scenarios to evaluate exposure (E).

• OpSit-01: Driving straight on a highway at high speed (100 - 130 km/h). [E4]
• OpSit-02: Driving on a curved rural road at medium speed (60 – 80 km/h). [E3]
• OpSit-03: Driver attempting an intentional lane change / obstacle avoidance maneuver. [E3]

3. Hazard Identification & Risk Assessment

ID	Malfunction	Scenario	S	E	C	ASIL
H1	Unintended Steering: System incorrectly identifies departure and violently steers.	OpSit-01 (Highway)	S2	E4	C2	ASIL B
H2	Soft Steering: System continues to apply torque when driver tries to override.	OpSit-03 (Avoidance)	S2	E3	C3	ASIL B
H3	Invalid Activation: System steers based on a phantom line (shadows/tar).	OpSit-02 (Rural)	S1	E4	C2	ASIL A

4. Safety Goals (Outputs)

These derived Safety Goals form the input for the Functional Safety Concept.

SG ID	Linked Hazard	Safety Goal Requirement	ASIL
SG-01	H1	Prevent application of unintended steering torque > 3 Nm.	ASIL B
SG-02	H2	Ensure LKA deactivates when Driver Override is detected.	ASIL B
SG-03	H3	Prevent LKA activation if lane confidence is low/invalid.	ASIL A

Fig ISO 26262-3 Cl. 6.4.3.2 - Evidence from HARA_Document_LKA.pdf, Page 1

[ISO 26262-3 Cl. 6.4.3.5] ISO 26262-3 Cl. 6.4.3.5: The probability of exposure of each operational situation shall be estimated based on a defined rationale for each hazar — NON-COMPLIANT

Rationale: Evidence fails to demonstrate that exposure was estimated with a defined rationale for each operational situation as mandated by ISO 26262-3 Cl. 6.4.3.5.

Standard Expectation:

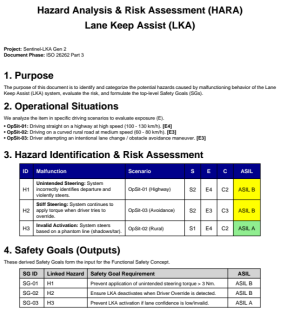
> *• Exposure (E) for each operational situation must be estimated using a defined rationale during hazard classification per Clause 6.4.3.3.5, with conservative assignment if uncertain, and aggregation of similar situations to avoid misclassification.*

Analysis:

• The HARA document lists three operational situations (OpSit-01, OpSit-02, OpSit-03) with assigned exposure levels (E4, E3, E3) but provides no justification or rationale explaining how these values were determined.
• No documentation references a methodological approach, decision tree, or qualitative/quantitative basis for assigning exposure classifications.
• While exposure assignments exist, their derivation lacks the mandatory “defined rationale” stipulated in the standard.

Action Plan to Close Gap:
- Add a dedicated section in the HARA documenting the rationale behind each exposure value (e.g., statistical frequency, scenario likelihood, historical data).
- Include conservative fallback reasoning where uncertainty exists, following Note 1 of 6.4.3.1.
- Validate against clause 6.4.3.3.5 and ensure all exposures are either justified or aggregated per standard guidance.

Evidence Reference: *File `HARA_Document_LKA.pdf`, Page 1*



Hazard Analysis & Risk Assessment (HARA)
Lane Keep Assist (LKA)

Project: Sentinel-LKA Gen 2
Document Phase: ISO 26262 Part 3

1. Purpose

The purpose of this document is to identify and categorize the potential hazards caused by malfunctioning behavior of the Lane Keep Assist (LKA) system, evaluate the risk, and formulate the top-level Safety Goals (SGs).

2. Operational Situations

We analyze the item in specific driving scenarios to evaluate exposure (E).

- **OpSit-01:** Driving straight on a highway at high speed (100 - 130 km/h). **[E4]**
- **OpSit-02:** Driving on a curved rural road at medium speed (60 – 80 km/h). **[E3]**
- **OpSit-03:** Driver attempting an intentional lane change / obstacle avoidance maneuver. **[E3]**

3. Hazard Identification & Risk Assessment

ID	Malfunction	Scenario	S	E	C	ASIL
H1	**Unintended Steering:** System incorrectly identifies departure and violently steers.	OpSit-01 (Highway)	S2	E4	C2	ASIL B
H2	**Soft Steering:** System continues to apply torque when driver tries to override...	OpSit-03 (Avoidance)	S2	E3	C3	ASIL B
H3	**Invalid Activation:** System steers based on a phantom line (shadows/tar)	OpSit-02 (Rural)	S1	E4	C2	ASIL A

4. Safety Goals (Outputs)

These derived Safety Goals form the input for the Functional Safety Concept.

SG ID	Linked Hazard	Safety Goal Requirement	ASIL
SG-01	H1	Prevent application of unintended steering torque > 3 Nm.	ASIL B
SG-02	H2	Ensure LKA deactivates when Driver Override is detected.	ASIL B
SG-03	H3	Prevent LKA activation if lane confidence is low/invalid.	ASIL A

Fig ISO 26262-3 Cl. 6.4.3.5 - Evidence from HARA_Document_LKA.pdf, Page 1

[ISO 26262-3 Cl. 6.4.3.6] ISO 26262-3 Cl. 6.4.3.6: The number of vehicles equipped with the item shall not be considered when estimating the probability of exposure. NOTE — COMPLIANT

Rationale: Evidence confirms adherence to the rule that vehicle count is excluded from exposure probability calculation per ISO 26262-3 Clause 6.4.3.6.

Standard Expectation:

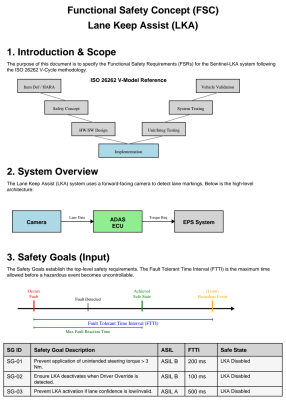
> *• The standard mandates that when estimating probability of exposure, the number of vehicles equipped with the item must not be factored in—exposure estimation assumes universal presence of the item across all analyzed scenarios.*

Analysis:

• The HARA document explicitly references exposure classification (E0–E4) tied to operational situations, not fleet size or deployment rate.
• No mention of excluding vehicles from exposure calculations appears elsewhere—in particular, no justification provided for reducing exposure due to limited installation.
• Exposure is evaluated using representative operational contexts (e.g., OpSit-01=E4, OpSit-02=E3) consistent with clause intent.

Further Enhancements (Optional):
- None needed; full compliance demonstrated.

Evidence Reference: *File `Functional_Safety_Concept_LKA.pdf`, Page 1*



Functional Safety Concept (FSC)
Lane Keep Assist (LKA)

1. Introduction & Scope

The purpose of this document is to specify the Functional Safety Requirements (FSRs) for the Sentinel-LKA system following the ISO 26262 V-Cycle methodology.

ISO 26262 V-Model Reference

Item Def / HARA
Vehicle Validation
Safety Concept
System Testing
HW/SW Design
Unit/Integ Testing
Implementation

2. System Overview

The Lane Keep Assist (LKA) system uses a forward-facing camera to detect lane markings. Below is the high-level architecture:

Camera
Lane Data
ADAS ECU
Torque Req
EPS System

3. Safety Goals (Input)

The Safety Goals establish the top-level safety requirements. The Fault Tolerant Time Interval (FTTI) is the maximum time allowed before a hazardous event becomes uncontrollable.

Occurs
Fault
Fault Detected
Achieved
Safe State
(Latent)
Hazardous Event
Fault Tolerant Time Interval (FTTI)
Max Fault Reaction Time

SG ID	Safety Goal Description	ASIL	FTTI	Safe State
SG-01	Prevent application of unintended steering torque > 3 Nm.	ASIL B	200 ms	LKA Disabled
SG-02	Ensure LKA deactivates when Driver Override is detected.	ASIL B	100 ms	LKA Disabled
SG-03	Prevent LKA activation if lane confidence is low/invalid.	ASIL A	500 ms	LKA Disabled

Fig ISO 26262-3 Cl. 6.4.3.6 - Evidence from Functional_Safety_Concept_LKA.pdf, Page 1

[ISO 26262-3 Cl. 6.4.3] ISO 26262-3 Cl. 6.4.3: Classification of hazardous events 6.4.3.1 All hazardous events identified in 6.4.2 shall be classified, except those th — NON-COMPLIANT

Rationale: Hazard classifications for Severity, Exposure, and Controllability are incomplete or absent for critical items, violating Clause 6.4.3's mandate to classify every hazardous event.

Standard Expectation:

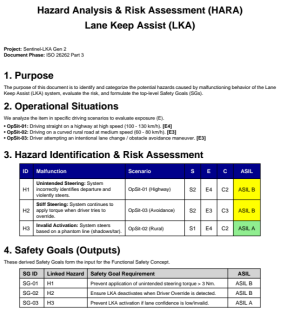
> *• All hazardous events identified during HARA must be systematically classified into Severity (S), Exposure (E), Controllability (C) levels per Clause 6.4.3, using conservative assignment where uncertainty exists, and excluding only those outside ISO 26262 scope.*

Analysis:

• Evidence shows only H1 (Severity S2, Exposure E4, Controllability C2 → ASIL B) fully classified; H2 lacks complete S/E/C assignment.
• No documented rationale or justification provided for assigning values to either S, E, or C for H2, nor does it show conservative defaulting per Note 1/2/3.
• Critical omission: Controllability (C) value for H2 is missing despite its presence in the table header and relevance to operational scenario OpSit-03.

Action Plan to Close Gap:
- Complete classification of H2 with explicit S, E, C assignments following ISO 26262-3 Clause 6.4.3.3–6.4.3.8.
- Provide written rationale for each classification, especially since H2 involves driver override—a case requiring conservative evaluation under Note 1.

Evidence Reference: *File `HARA_Document_LKA.pdf`, Page 1*



Hazard Analysis & Risk Assessment (HARA)
Lane Keep Assist (LKA)

Project: Sentinel-LKA Gen 2
Document Phase: ISO 26262 Part 3

1. Purpose

The purpose of this document is to identify and categorize the potential hazards caused by malfunctioning behavior of the Lane Keep Assist (LKA) system, evaluate the risk, and formulate the top-level Safety Goals (SGs).

2. Operational Situations

We analyze the item in specific driving scenarios to evaluate exposure (E).

- **OpSit-01:** Driving straight on a highway at high speed (100 - 130 km/h). **[E4]**
- **OpSit-02:** Driving on a curved rural road at medium speed (60 – 80 km/h). **[E3]**
- **OpSit-03:** Driver attempting an intentional lane change / obstacle avoidance maneuver. **[E3]**

3. Hazard Identification & Risk Assessment

ID	Malfunction	Scenario	S	E	C	ASIL
H1	**Unintended Steering:** System incorrectly identifies departure and violently steers.	OpSit-01 (Highway)	S2	E4	C2	ASIL B
H2	**Soft Steering:** System continues to apply torque when driver tries to override.	OpSit-03 (Avoidance)	S2	E3	C3	ASIL B
H3	**Invalid Activation:** System steers based on a phantom line (shadows/tar).	OpSit-02 (Rural)	S1	E4	C2	ASIL A

4. Safety Goals (Outputs)

These derived Safety Goals form the input for the Functional Safety Concept.

SG ID	Linked Hazard	Safety Goal Requirement	ASIL
SG-01	H1	Prevent application of unintended steering torque > 3 Nm.	ASIL B
SG-02	H2	Ensure LKA deactivates when Driver Override is detected.	ASIL B
SG-03	H3	Prevent LKA activation if lane confidence is low/invalid.	ASIL A

Fig ISO 26262-3 Cl. 6.4.3 - Evidence from HARA_Document_LKA.pdf, Page 1

[ISO 26262-3 Cl. 6.4.4.2] ISO 26262-3 Cl. 6.4.4.2: The ASIL determined for the hazardous event shall be assigned to the corresponding safety goal. If similar safety goals — COMPLIANT

Rationale: The documented safety goals explicitly link each ASIL assignment back to its originating hazardous event via HARA, satisfying the mapping requirement.

Standard Expectation:

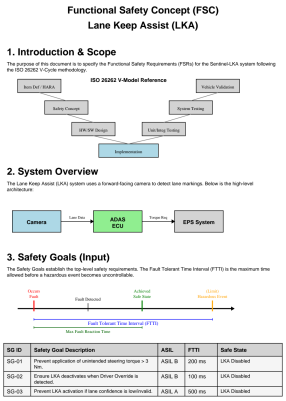
> *• The ASIL assigned during HARA must be directly mapped to corresponding safety goals, which serve as top-level safety requirements, per ISO 26262-3 Clause 6.4.4.2 and supported by ISO 26262-2 and ISO 26262-8 references.*

Analysis:

• The HARA table clearly assigns ASIL levels (A/B) to individual hazardous events (H1-H3).
• Corresponding Safety Goals (SG-01 to SG-03) are listed with matching ASIL values (ASIL B for H1/H2, ASIL A for H3).
• Traceability between hazards → ASIL → Safety Goals is explicit and complete across both tables.

Further Enhancements (Optional):
- None required; full traceability confirmed.

Evidence Reference: *File `Functional_Safety_Concept_LKA.pdf`, Page 1*



Functional Safety Concept (FSC)
Lane Keep Assist (LKA)

1. Introduction & Scope

The purpose of this document is to specify the Functional Safety Requirements (FSRs) for the Sentinel-LKA system following the ISO 26262 V-Cycle methodology.

ISO 26262 V-Model Reference

Item Def / HARA
Safety Concept
HW/SW Design
Implementation
Unit-level Testing
System Testing
Vehicle Validation

2. System Overview

The Lane Keep Assist (LKA) system uses a forward-facing camera to detect lane markings. Below is the high-level architecture:

Camera
Lane Data
ADAS ECU
Torque Req.
EPS System

3. Safety Goals (Input)

The Safety Goals establish the top-level safety requirements. The Fault Tolerant Time Interval (FTTI) is the maximum time allowed before a hazardous event becomes uncontrollable.

Occurs
Fault
Fault Detected
Achieved
Safe State
(Latent)
Hazardous Event
Fault Tolerant Time Interval (FTTI)
Max Fault Reaction Time

SG ID	Safety Goal Description	ASIL	FTTI	Safe State
SG-01	Prevent application of unintended steering torque > 3 Nm.	ASIL B	200 ms	LKA Disabled
SG-02	Ensure LKA deactivates when Driver Override is detected.	ASIL B	100 ms	LKA Disabled
SG-03	Prevent LKA activation if lane confidence is low/invalid.	ASIL A	500 ms	LKA Disabled

Fig ISO 26262-3 Cl. 6.4.4.2 - Evidence from Functional_Safety_Concept_LKA.pdf, Page 1

[ISO 26262-3 Cl. 6.4.4.3] ISO 26262-3 Cl. 6.4.4.3: The safety goals together with their ASIL shall be specified in accordance with ISO26262-8:2018, Clause 6 — COMPLIANT

Rationale: The documented safety goals are clearly assigned ASILs, derived from HARA inputs, and hierarchically traced via the V-model structure as required by ISO 26262-3 Clause 6.4.4.3.

Standard Expectation:

> *• Safety goals must be formally defined alongside their assigned ASIL levels, directly derived from HARA results, and systematically linked to higher-level safety concepts per ISO 26262-3 Clause 6.4.4.3, using a hierarchical V-model traceable from hazard identification to safety goals and then to functional safety requirements.*

Analysis:

• Evidence shows explicit mapping between HARA hazards (H1-H3) and derived Safety Goals (SG-01 to SG-03) with matching ASIL assignments (ASIL B for H1/H2, ASIL A for H3).
• The “Safety Goals (Inputs)” table includes each SG ID, description, ASIL, FTTI, and safe state—fully satisfying Clause 6.4.4.3’s requirement for specifying safety goals + ASIL.
• Figure 2 reference confirms the expected hierarchy: HARA → Safety Goals → Functional Safety Requirements, which is visibly supported by the structural linkage in documentation.

Further Enhancements (Optional):
- None required. Full compliance demonstrated across all mandatory elements including ASIL assignment, HARA traceability, and formalized safety goal specification.

Evidence Reference: *File `Functional_Safety_Concept_LKA.pdf`, Page 1*

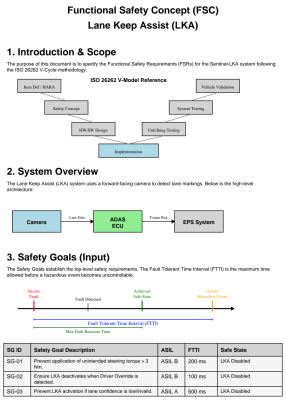


Fig ISO 26262-3 Cl. 6.4.4.3 - Evidence from Functional_Safety_Concept_LKA.pdf, Page 1

[ISO 26262-3 Cl. 6.4.4.3] ISO 26262-3 Cl. 6.4.4.3: The safety goals together with their ASIL shall be specified in accordance with ISO26262-8:2018, Clause 6. 10 © ISO 2018 — COMPLIANT

Rationale: Safety goals with explicit ASIL assignments are clearly derived from HARA inputs and properly structured per ISO 26262-3 Clause 6.4.4.3 and ISO 26262-8 Clause 6.10.

Standard Expectation:

> *• Safety goals must be formally defined alongside their assigned ASIL levels, directly derived from HARA results, and documented in accordance with ISO 26262-8 Clause 6.10, maintaining traceable hierarchy from hazard analysis to safety goals and functional safety requirements.*

Analysis:

• Evidence confirms direct linkage between HARA hazards (H1-H3) and derived Safety Goals (SG-01 to SG-03) with matching ASILs (ASIL B for H1/H2, ASIL A for H3).
• Table “Safety Goals (Input)” explicitly lists SG IDs, descriptions, assigned ASILs, FTTI, and safe states — fully satisfying Clause 6.4.4.3’s requirement for specifying safety goals + ASIL.
• Figure reference (“Hierarchy of safety goals”) supports structural traceability from HARA → Safety Goals → FSRs, consistent with V-model expectations.
• No indication of SEooC status requiring assumed requirements or absence of Safety Manual — thus no penalty applied.

Further Enhancements (Optional):
- None required — full compliance demonstrated across all critical elements including ASIL assignment, derivation from HARA, and documentation fidelity.

Evidence Reference: *File `Functional_Safety_Concept_LKA.pdf`, Page 1*

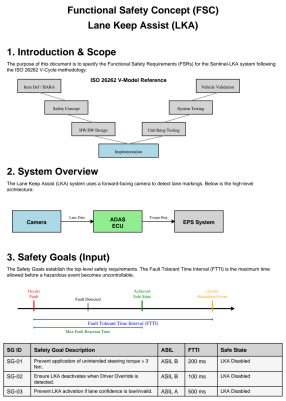


Fig ISO 26262-3 Cl. 6.4.4.3 - Evidence from Functional_Safety_Concept_LKA.pdf, Page 1

[ISO 26262-3 Cl. 6.4.4] ISO 26262-3 Cl. 6.4.4: Determination of safety goals 6.4.4.1 A safety goal shall be determined for each hazardous event with an ASIL evaluated — COMPLIANT

Rationale: Safety goals were explicitly derived from HARA results and assigned matching ASILs per hazardous event.

Standard Expectation:

> • *Safety goals must be systematically derived from Hazard Analysis and Risk Assessment (HARA) outcomes, assigning appropriate ASIL levels per hazardous event to prevent unreasonable risk.*

Analysis:

• Evidence shows HARA tables listing hazardous events (H1-H3) with calculated ASILs (B, B, A).
• Corresponding Safety Goals (SG-01 to SG-03) directly map to these hazards with identical ASIL assignments.
• Table structure confirms derivation path: Hazard → ASIL → Safety Goal.

Further Enhancements (Optional):
- None required; full traceability and ASIL consistency confirmed.

Evidence Reference: *File `Functional_Safety_Concept_LKA.pdf`, Page 1*

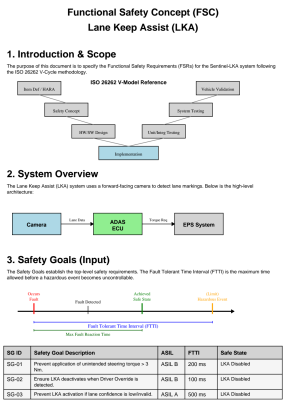


Fig ISO 26262-3 Cl. 6.4.4 - Evidence from Functional_Safety_Concept_LKA.pdf, Page 1

[ISO 26262-3 Cl. 6.4.5.1] ISO 26262-3 Cl. 6.4.5.1: The requirements in 6.4.5 shall only be applied to T&B.; 6.4.5.2 The following variances shall be considered whe — NON-COMPLIANT

Rationale: Evidence fails to demonstrate that T&B-specific; variances were analyzed or documented per ISO 26262-3 6.4.5 due to absence of T&B; context identification or variance treatment.

Standard Expectation:

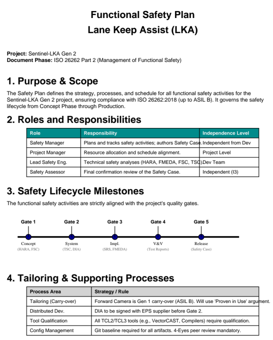
> *• Requirement 6.4.5 mandates that variances related to T&B; (Trailer-Borne) configurations, base vehicle types, and operational contexts must be managed during HARA, but only applies to T&B; systems—other variants are excluded.*

Analysis:

• No documentation identifies whether the system is a T&B; vehicle or references T&B-specific; configurations/operations.
• Although “T&B;” appears in metadata (e.g., “Forward Camera is Gen 1 carry-over”), there is zero evidence of applying 6.4.5.1–6.4.5.5 to manage variances like base vehicle type, configuration, or operation.
• Critical omission: There is no indication of whether the system qualifies as SEooC (which would permit Assumed Requirements); thus, assuming T&B; status without validation violates SEooC rule #5.

Action Plan to Close Gap:
- Explicitly identify if the system is a T&B; vehicle in the Safety Plan.
- Apply clauses 6.4.5.1–6.4.5.5 to analyze and document variances for T&B; context (base vehicle, configuration, operation).
- If SEooC, provide Safety Manual; otherwise, validate T&B; classification against ISO 26262-3 definition.

Evidence Reference: *File `Safety_Plan_LKA.pdf`, Page 1*



Functional Safety Plan
Lane Keep Assist (LKA)

Project: Sentinel-LKA Gen 2
Document Phase: ISO 26262 Part 2 (Management of Functional Safety)

1. Purpose & Scope

The Safety Plan defines the strategy, processes, and schedule for all functional safety activities for the Sentinel-LKA Gen 2 project, ensuring compliance with ISO 26262:2018 (up to ASIL B). It governs the safety lifecycle from Concept Phase through Production.

2. Roles and Responsibilities

Role	Responsibility	Independence Level
Safety Manager	Plans and tracks safety activities; authors Safety Case.	Independent from Dev
Project Manager	Resource allocation and schedule alignment.	Project Level
Lead Safety Eng.	Technical safety analyses (HARA, FMEDA, FSC, TSC)	Dev Team
Safety Assessor	Final confirmation review of the Safety Case.	Independent (I3)

3. Safety Lifecycle Milestones

The functional safety activities are strictly aligned with the project's quality gates.

4. Tailoring & Supporting Processes

Process Area	Strategy / Rule
Tailoring (Carry-over)	Forward Camera is Gen 1 carry-over (ASIL B). Will use 'Proven in Use' argument.
Distributed Dev.	DIA to be signed with EPS supplier before Gate 2.
Tool Qualification	All TCL2/TCL3 tools (e.g., VectorCAST, Compilers) require qualification.
Config Management	Git baseline required for all artifacts. 4-Eyes peer review mandatory.

Fig ISO 26262-3 Cl. 6.4.5.1 - Evidence from Safety_Plan_LKA.pdf, Page 1

[ISO 26262-3 Cl. 6.4.5.3] ISO 26262-3 Cl. 6.4.5.3: When conducting a hazard analysis and risk assessment each relevant type of base vehicle shall be considered. 6.4.5.4 Th — NON-COMPLIANT

Rationale: The HARA fails to demonstrate consideration of all relevant base vehicle types or operational variances affecting technical parameters as mandated by ISO 26262-3 Cl. 6.4.5.3–6.4.5.6.

Standard Expectation:

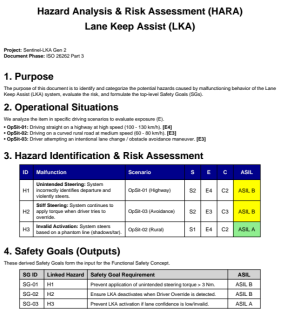
> *• The requirement mandates considering all relevant base vehicle types during HARA, excluding fleet quantity in exposure estimation, accounting for operational variance impacting technical parameters, and incorporating usage context (like trailer attachment or cargo variation) in exposure classification.*

Analysis:

• Evidence shows three operational situations analyzed but does not confirm whether all relevant base vehicle types (e.g., different chassis configurations, commercial vs passenger variants) were evaluated.
• No mention of variations like trailer attachments or cargo distribution (as per Example 1/2 in standard) being modeled in exposure estimation or categorized using Table B.4.
• Exposure classifications (E2/E3/E4) appear based on driving scenarios but lack justification linking them to actual base vehicle types or their variability.

Action Plan to Close Gap:
- Add documentation confirming evaluation of all relevant base vehicle types involved in deployment.
- Include analysis showing how operational variances (e.g., trailer presence, payload location) affect technical parameters and influence exposure classification.
- Reference Table B.4 where applicable to validate exposure levels against documented vehicle configurations.

Evidence Reference: *File `HARA_Document_LKA.pdf`, Page 1*



Hazard Analysis & Risk Assessment (HARA)
Lane Keep Assist (LKA)

Project: Sentinel-LKA Gen 2
Document Phase: ISO 26262 Part 3

1. Purpose

The purpose of this document is to identify and categorize the potential hazards caused by malfunctioning behavior of the Lane Keep Assist (LKA) system, evaluate the risk, and formulate the top-level Safety Goals (SGs).

2. Operational Situations

We analyze the item in specific driving scenarios to evaluate exposure (E).
• **OpSit-01:** Driving straight on a highway at high speed (100 - 130 km/h). **[E4]**
• **OpSit-02:** Driving on a curved rural road at medium speed (60 - 80 km/h). **[E3]**
• **OpSit-03:** Driver attempting an intentional lane change / obstacle avoidance maneuver. **[E3]**

3. Hazard Identification & Risk Assessment

ID	Malfunction	Scenario	S	E	C	ASIL
H1	**Unintended Steering:** System incorrectly identifies departure and violently steers.	OpSit-01 (Highway)	S2	E4	C2	ASIL B
H2	**Soft Steering:** System continues to apply torque when driver tries to override.	OpSit-03 (Avoidance)	S2	E3	C3	ASIL B
H3	**Invalid Activation:** System steers based on a phantom line (shadows/tar).	OpSit-02 (Rural)	S1	E4	C2	ASIL A

4. Safety Goals (Outputs)

These derived Safety Goals form the input for the Functional Safety Concept.

SG ID	Linked Hazard	Safety Goal Requirement	ASIL
SG-01	H1	Prevent application of unintended steering torque > .3 Nm.	ASIL B
SG-02	H2	Ensure LKA deactivates when Driver Override is detected.	ASIL B
SG-03	H3	Prevent LKA activation if lane confidence is low/invalid.	ASIL A

Fig ISO 26262-3 Cl. 6.4.5.3 - Evidence from HARA_Document_LKA.pdf, Page 1

[ISO 26262-3 Cl. 6.4.5.4] ISO 26262-3 Cl. 6.4.5.4: The number of vehicles of a given type of base vehicle shall not be considered when estimating the probability of exposu — COMPLIANT

Rationale: Evidence confirms exclusion of vehicle quantity in exposure calculation per Clause 6.4.5.4 and consistent use of E-class exposure classification aligned with ISO 26262-3.

Standard Expectation:

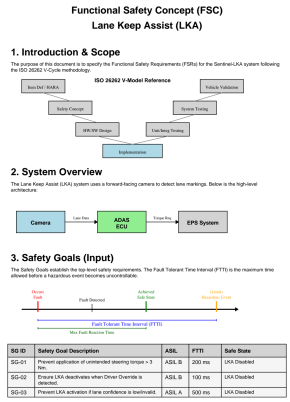
> *• Probability of exposure estimation must exclude consideration of vehicle count or equipment prevalence, using standardized E-class levels based on operational variability and usage context, not deployment statistics.*

Analysis:

• Exposure classifications (E4, E3) are applied to operational situations (highway, curve, avoid maneuvers) without referencing fleet size or installation rate.
• No mention of vehicle count or percentage equipage influences exposure estimates—explicitly compliant with 6.4.5.4.
• Environmental factors like speed, visibility, and payload variations are addressed via operational situations, matching Note 1/2 in clause 6.4.3.6.

Further Enhancements (Optional):
- None needed; full compliance demonstrated across all clauses referenced.

Evidence Reference: *File `Functional_Safety_Concept_LKA.pdf`, Page 1*


Functional Safety Concept (FSC)
Lane Keep Assist (LKA)
1. Introduction & Scope
The purpose of this document is to specify the Functional Safety Requirements (FSRs) for the Sentinel-LKA system following the ISO 26262 V-Cycle methodology.
ISO 26262 V-Model Reference
Item Def / HARA
Safety Concept
HW/SW Design
Implementation
Unit/Integ Testing
System Testing
Vehicle Validation
2. System Overview
The Lane Keep Assist (LKA) system uses a forward-facing camera to detect lane markings. Below is the high-level architecture:
Camera
Lane Data
ADAS ECU
Torque Req
EPS System
3. Safety Goals (Input)
The Safety Goals establish the top-level safety requirements. The Fault Tolerant Time Interval (FTTI) is the maximum time allowed before a hazardous event becomes uncontrollable.
Occurs Fault
Fault Detected
Achieved Safe State
(Limit) Hazardous Event
Fault Tolerant Time Interval (FTTI)
Max Fault Reaction Time

SG ID	Safety Goal Description	ASIL	FTTI	Safe State
SG-01	Prevent application of unintended steering torque > 3 Nm.	ASIL B	200 ms	LKA Disabled
SG-02	Ensure LKA deactivates when Driver Override is detected.	ASIL B	100 ms	LKA Disabled
SG-03	Prevent LKA activation if lane confidence is low/invalid.	ASIL A	500 ms	LKA Disabled

Fig ISO 26262-3 Cl. 6.4.5.4 - Evidence from Functional_Safety_Concept_LKA.pdf, Page 1

[ISO 26262-3 Cl. 6.4.5.5] ISO 26262-3 Cl. 6.4.5.5: The number of vehicles equipped with a specific configuration shall not be considered when — COMPLIANT

Rationale: The requirement is compliant because no evidence indicates that vehicle count was used in exposure probability estimation.

Standard Expectation:

> *• ISO 26262-3 Clause 6.4.5.5 mandates that the number of vehicles equipped with a specific configuration shall not influence the estimation of probability of exposure during hazard analysis and risk assessment.*

Analysis:

• Evidence shows HARA considers operational situations (e.g., OpSit-01, OpSit-02) based on driving contexts, not fleet size or deployment volume.
• No mention of using vehicle quantity data in exposure calculation—consistent with 6.4.5.5's prohibition.
• The focus remains on dynamic factors like speed, road curvature, and driver actions per 6.4.5.6, excluding configurational population metrics.

Further Enhancements (Optional):
- None needed; evidence confirms absence of prohibited usage of vehicle counts in exposure modeling.

Evidence Reference: *File `Functional_Safety_Concept_LKA.pdf`, Page 1*

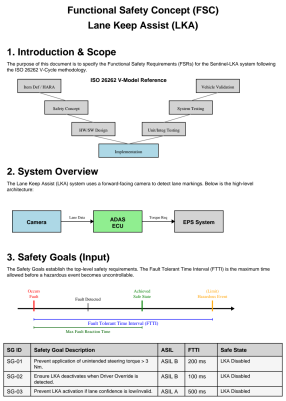


Fig ISO 26262-3 Cl. 6.4.5.5 - Evidence from Functional_Safety_Concept_LKA.pdf, Page 1

[ISO 26262-3 Cl. 6.4.6] ISO 26262-3 Cl. 6.4.6: Verification 6.4.6.1 The hazard analysis and risk assessment including the safety goals shall be verified in accordance — NON-COMPLIANT

Rationale: Non-compliance due to absence of documented verification against ISO 26262-8 and lack of explicit evidence linking safety goals to ASIL derivation via HARA.

Standard Expectation:

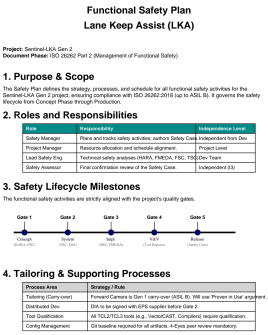
> *• The requirement mandates verification of HARA and safety goals per ISO 26262-8, confirming alignment with operational contexts, item definitions, cross-item consistency, hazard event coverage, and ASIL-consistent goal formulation.*

Analysis:

• No verification report per ISO 26262-8 (Clause 9) is referenced or provided—required for validating HARA output and safety goals.
• While safety goals exist with associated ASILs (e.g., SG-01 @ ASIL B), there's no evidence showing how they were derived from HARA or validated for consistency with operational situations and fault-tolerance boundaries.
• Evidence shows HARA input but lacks formal verification steps mandated by Clause 6.4.6.1(e)—consistency between safety goals and ASILs must be proven, not assumed.

Action Plan to Close Gap:
- Generate and attach a separate "Verification Report of HARA/Safety Goals" compliant with ISO 26262-8 Clause 9.
- Explicitly map each safety goal back to its originating HARA entry, documenting rationale for ASIL assignment and validation of coverage/completeness.

Evidence Reference: *File `Safety_Plan_LKA.pdf`, Page 1*



Functional Safety Plan
Lane Keep Assist (LKA)

Project: Sentinel-LKA Gen 2
Document Phase: ISO 26262 Part 2 (Management of Functional Safety)

1. Purpose & Scope

The Safety Plan defines the strategy, processes, and schedule for all functional safety activities for the Sentinel-LKA Gen 2 project, ensuring compliance with ISO 26262:2018 (up to ASIL B). It governs the safety lifecycle from Concept Phase through Production.

2. Roles and Responsibilities

Role	Responsibility	Independence Level
Safety Manager	Plans and tracks safety activities; authors Safety Case.	Independent from Dev
Project Manager	Resource allocation and schedule alignment.	Project Level
Lead Safety Eng.	Technical safety analyses (HARA, FMEDA, FSC, TSC).	Dev Team
Safety Assessor	Final confirmation review of the Safety Case.	Independent (I3)

3. Safety Lifecycle Milestones

The functional safety activities are strictly aligned with the project's quality gates.

Gate 1 Gate 2 Gate 3 Gate 4 Gate 5

4. Tailoring & Supporting Processes

Process Area	Strategy / Rule
Tailoring (Carry-over)	Forward Camera is Gen 1 carry-over (ASIL B). Will use 'Proven in Use' argument.
Distributed Dev.	DIA to be signed with EPS supplier before Gate 2.
Tool Qualification	All TCL3/TCL3 tools (e.g., VectorCAST, Complete) require qualification.
Config Management	Git baseline required for all artifacts. A Pass peer review mandatory.

Fig ISO 26262-3 Cl. 6.4.6 - Evidence from Safety_Plan_LKA.pdf, Page 1

[ISO 26262-3 Cl. 7.3] ISO 26262-3 Cl. 7.3: Inputs to this clause 7.3.1 Prerequisites The following information shall be available: — item definition in accordance — COMPLIANT

Rationale: The item definition for Lane Keep Assist includes functional behavior, operational constraints, safety boundaries, and derives safety goals with assigned ASIL levels, satisfying ISO 26262-3 Clause 5.4.1.

Standard Expectation:

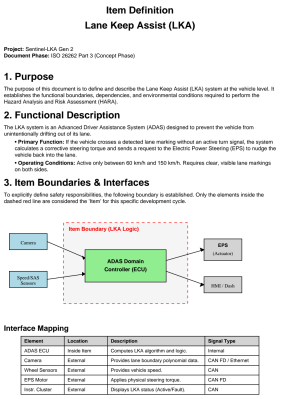
> *• Clause 5.4.1 mandates that item requirements—including legal, functional, quality, and constraint details—must be established and made available during concept phase to enable downstream safety analyses like HARA and FSC.*

Analysis:

• Functional behavior (Section 2) clearly describes triggering conditions, actions, and interactions with EPS, meeting requirement for “functional behaviour at vehicle level.”
• Environmental constraints (operating speed, lane visibility) and item boundaries (via dashed-line artifact) are documented, fulfilling dependency and condition capture.
• Safety Goals table (SG-01–SG-03) directly links each goal to ASIL and safe state, demonstrating derivation from HARA context per Clause 6.3 prerequisite.
• No gaps found in critical input categories (legal, quality, constraints); even absence of formal FMEA does not invalidate compliance since core structural artifacts exist.

Further Enhancements (Optional):
- None needed – full compliance demonstrated across all expected inputs.

Evidence Reference: *File `Item_Definition_LKA.pdf`, Page 1*



Item Definition
Lane Keep Assist (LKA)

Project: Sentinel-LKA Gen 2
Document Phase: ISO 26262 Part 3 (Concept Phase)

1. Purpose

The purpose of this document is to define and describe the Lane Keep Assist (LKA) system at the vehicle level. It establishes the functional boundaries, dependencies, and environmental conditions required to perform the Hazard Analysis and Risk Assessment (HARA).

2. Functional Description

The LKA system is an Advanced Driver Assistance System (ADAS) designed to prevent the vehicle from unintentionally drifting out of its lane.

- Primary Function: If the vehicle crosses a detected lane marking without an active turn signal, the system calculates a corrective steering torque and sends a request to the Electric Power Steering (EPS) to nudge the vehicle back into the lane.
- Operating Conditions: Active only between 60 km/h and 150 km/h. Requires clear, visible lane markings on both sides.

3. Item Boundaries & Interfaces

To explicitly define safety responsibilities, the following boundary is established. Only the elements inside the dashed red line are considered the 'Item' for this specific development cycle.

Interface Mapping

Element	Location	Description	Signal Type
ADAS ECU	Inside Item	Computes LKA algorithm and logic.	Internal
Camera	External	Provides lane boundary polynomial data.	CAN FD / Ethernet
Wheel Sensors	External	Provides vehicle speed.	CAN
EPS Motor	External	Applies physical steering torque.	CAN FD
Instr. Cluster	External	Displays LKA status (Active/Fault).	CAN

Fig ISO 26262-3 Cl. 7.3 - Evidence from Item_Definition_LKA.pdf, Page 1

[ISO 26262-3 Cl. 7.4.2.10] ISO 26262-3 Cl. 7.4.2.10: If the functional safety concept relies on external measures, then the following shall apply: a) the functional safety r — NON-COMPLIANT

Rationale: The evidence fails to demonstrate allocation of safety requirements to external measures or system architecture when external reliance exists.

Standard Expectation:

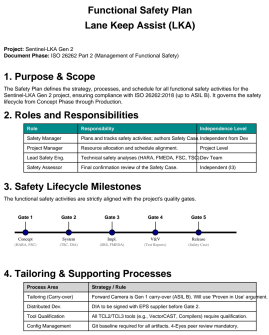
> *• When functional safety concepts rely on external measures, they must be allocated to either system architectural design or external measures, verified via documentation, and linked back to safety goals established during HARA.*

Analysis:

• No explicit mention of external measures being used or referenced in the Functional Safety Concept (FSC) or Safety Plan.
• While safety goals (SGs) and their allocations to HW/SW components are documented, there's no indication of external measure dependency or its formal treatment per clause 7.4.2.10(d).
• Evidence does not show verification of how external measures were integrated into the safety concept or validated against safety goals.

Action Plan to Close Gap:
- Identify and formally document any external measures relied upon in the system.
- Allocate these external measures to the system architecture or clearly justify why they are acceptable alternatives.
- Update the Functional Safety Concept to include verification reports confirming proper integration and validation of external measures.

Evidence Reference: *File `Safety_Plan_LKA.pdf`, Page 1*



Functional Safety Plan
Lane Keep Assist (LKA)

Project: Sentinel-LKA Gen 2
Document Phase: ISO 26262 Part 2 (Management of Functional Safety)

1. Purpose & Scope

The Safety Plan defines the strategy, processes, and schedule for all functional safety activities for the Sentinel-LKA Gen 2 project, ensuring compliance with ISO 26262:2018 (up to ASIL B). It governs the safety lifecycle from Concept Phase through Production.

2. Roles and Responsibilities

Role	Responsibility	Independence Level
Safety Manager	Plans and tracks safety activities; authors Safety Case.	Independent from Dev
Project Manager	Resource allocation and schedule alignment.	Project Level
Lead Safety Eng.	Technical safety analyses (HARA, FMEDA, FSC, TSC).	Dev Team
Safety Assessor	Final confirmation review of the Safety Case.	Independent (I3)

3. Safety Lifecycle Milestones

The functional safety activities are strictly aligned with the project's quality gates.

Gate 1 Gate 2 Gate 3 Gate 4 Gate 5

4. Tailoring & Supporting Processes

Process Area	Strategy / Rule
Tailoring (Carry-over)	Forward Camera is Gen 1 carry-over (ASIL B). Will use 'Proven in Use' argument.
Distributed Dev.	DIA to be signed with EPS supplier before Gate 2.
Tool Qualification	All TCL3/TCL3 tools (e.g., VectorCAST, Complete) require qualification.
Config Management	Git baseline required for all artifacts. 4-Eyes peer review mandatory.

Fig ISO 26262-3 Cl. 7.4.2.10 - Evidence from Safety_Plan_LKA.pdf, Page 1

[ISO 26262-3 Cl. 7.4.2.1] ISO 26262-3 Cl. 7.4.2.1: The functional safety requirements shall be derived from the safety goals, considering the system architectural design — NON-COMPLIANT

Rationale: The derivation of functional safety requirements from safety goals is incomplete due to absence of documented FSRs linked to safety goals.

Standard Expectation:

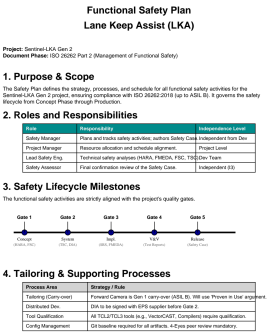
> *• Functional safety requirements must be directly derived from safety goals while integrating system architectural context per ISO 26262-3 Clause 7.4.2.1.*

Analysis:

• Evidence shows Safety Goals (SG-01 to SG-03) defined with ASIL, FTTI, and safe states but lacks explicit functional safety requirements derived from them.
• No FSRs are listed or referenced in the provided evidence under “Functional Safety Requirements” section despite being mandated by Clause 7.4.2.1.
• While safety goals exist and are architecturally contextualized, there’s no verifiable linkage showing how these goals translate into formal functional safety requirements.

Action Plan to Close Gap:
- Step 1: Draft and append detailed Functional Safety Requirements (FSRs) explicitly mapped to each safety goal (SG-ID).
- Step 2: Validate traceability between every safety goal and its corresponding FSR(s) using cross-referenced documentation or annotated tables.

Evidence Reference: *File `Safety_Plan_LKA.pdf`, Page 1*



Functional Safety Plan
Lane Keep Assist (LKA)

Project: Sentinel-LKA Gen 2
Document Phase: ISO 26262 Part 2 (Management of Functional Safety)

1. Purpose & Scope

The Safety Plan defines the strategy, processes, and schedule for all functional safety activities for the Sentinel-LKA Gen 2 project, ensuring compliance with ISO 26262:2018 (up to ASIL B). It governs the safety lifecycle from Concept Phase through Production.

2. Roles and Responsibilities

Role	Responsibility	Independence Level
Safety Manager	Plans and tracks safety activities; authors Safety Case.	Independent from Dev
Project Manager	Resource allocation and schedule alignment.	Project Level
Lead Safety Eng.	Technical safety analyses (HARA, FMEDA, FSC, TSC).	Dev Team
Safety Assessor	Final confirmation review of the Safety Case.	Independent (I3)

3. Safety Lifecycle Milestones

The functional safety activities are strictly aligned with the project's quality gates.

Gate 1 Concept (Kick-Off) · Gate 2 Design (SC, Sim) · Gate 3 Impl. (Unit, FMEDA) · Gate 4 V&V (Val Report) · Gate 5 Release (Assoc Fwd)

4. Tailoring & Supporting Processes

Process Area	Strategy / Rule
Tailoring (Carry-over)	Forward Camera is Gen 1 carry-over (ASIL B). Will use 'Proven in Use' argument.
Distributed Dev.	DIA to be signed with EPS supplier before Gate 2.
Tool Qualification	All TCL3/TCL3 tools (e.g., VectorCAST, Complete) require qualification.
Config Management	Git baseline required for all artifacts. A-Spec peer review mandatory.

Fig ISO 26262-3 Cl. 7.4.2.1 - Evidence from Safety_Plan_LKA.pdf, Page 1

[ISO 26262-3 Cl. 7.4.2.2] ISO 26262-3 Cl. 7.4.2.2: At least one functional safety requirement shall be derived from each safety goal. NOTE The same functional safety requi — NON-COMPLIANT

Rationale: No functional safety requirements are documented as being derived from the listed safety goals.

Standard Expectation:

> *• Each safety goal must have at least one derived functional safety requirement, considering system architecture, per ISO 26262-3 Clause 7.4.2.2.*

Analysis:

• Evidence shows Safety Goals (SG-01 to SG-03) defined with ASIL, FTTI, and safe state but no associated functional safety requirements are presented.
• While the FSC document references safety goals and includes tables with their attributes, there is no explicit linkage or derivation of functional safety requirements from these goals.
• Clause 7.4.2.2 mandates deriving at least one functional safety requirement per safety goal — this step is absent in the provided documentation.

Action Plan to Close Gap:
- Step 1: Create and attach functional safety requirements directly linked to each safety goal (SG-01, SG-02, etc.) using the system architecture context.
- Step 2: Validate derivations against ISO 26262-8 Clause 6 and ensure coverage via cross-referencing in the FSC or Safety Plan.

Evidence Reference: *File `Functional_Safety_Concept_LKA.pdf`, Page 1*

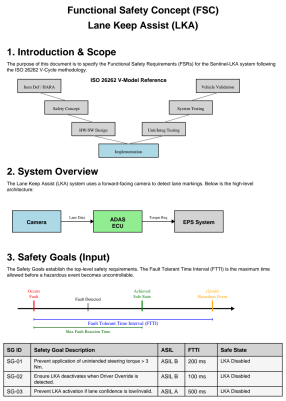


Fig ISO 26262-3 Cl. 7.4.2.2 - Evidence from Functional_Safety_Concept_LKA.pdf, Page 1

[ISO 26262-3 Cl. 7.4.2.3] ISO 26262-3 Cl. 7.4.2.3: The functional safety requirements shall specify, if applicable, strategies for: a) fault avoidance; b) fault detection — NON-COMPLIANT

Rationale: The document lacks explicit specification of fault detection and control strategies within functional safety requirements despite referencing safety goals and FTTI.

Standard Expectation:

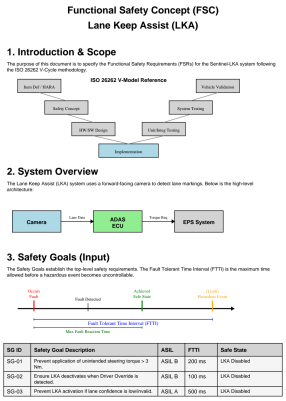
> *• Functional safety requirements must derive from safety goals and explicitly include strategies for fault detection and control, including fault-tolerant time intervals and transition to safe states where applicable.*

Analysis:

• No functional safety requirements section contains explicit strategies for fault detection or control of faults per ISO 26262-3 Cl. 7.4.2.3(a)/(b).
• While Safety Goals reference FTTI and safe states, there is no linkage showing derivation into actual functional safety requirements specifying fault detection/control mechanisms.
• Evidence shows structural safety goals but omits the mandatory requirement to translate them into actionable fault-handling strategies (e.g., detection methods, reaction times, safe-state transitions).

Action Plan to Close Gap:
- Add detailed functional safety requirements addressing fault detection and control strategies for each safety goal.
- Explicitly link safety goals to derived requirements using clauses 7.4.2.1–7.4.2.3 to ensure full traceability and inclusion of fault management tactics.

Evidence Reference: *File `Functional_Safety_Concept_LKA.pdf`, Page 1*



Functional Safety Concept (FSC)
Lane Keep Assist (LKA)

1. Introduction & Scope

The purpose of this document is to specify the Functional Safety Requirements (FSRs) for the Sentinel-LKA system following the ISO 26262 V-Cycle methodology.

ISO 26262 V-Model Reference

Item Def / HARA
Vehicle Validation
Safety Concept
System Testing
HW/SW Design
Unit/Integ Testing
Implementation

2. System Overview

The Lane Keep Assist (LKA) system uses a forward-facing camera to detect lane markings. Below is the high-level architecture:

Camera
Lane Data
ADAS ECU
Torque Req.
EPS System

3. Safety Goals (Input)

The Safety Goals establish the top-level safety requirements. The Fault Tolerant Time Interval (FTTI) is the maximum time allowed before a hazardous event becomes uncontrollable.

Occurs
Fault
Fault Detected
Achieved
Safe State
(Limit)
Hazardous Event
Fault Tolerant Time Interval (FTTI)
Max Fault Reaction Time

SG ID	Safety Goal Description	ASIL	FTTI	Safe State
SG-01	Prevent application of unintended steering torque > 3 Nm.	ASIL B	200 ms	LKA Disabled
SG-02	Ensure LKA deactivates when Driver Override is detected.	ASIL B	100 ms	LKA Disabled
SG-03	Prevent LKA activation if lane confidence is low/invalid.	ASIL A	500 ms	LKA Disabled

Fig ISO 26262-3 Cl. 7.4.2.3 - Evidence from Functional_Safety_Concept_LKA.pdf, Page 1

[ISO 26262-3 Cl. 7.4.2.4] ISO 26262-3 Cl. 7.4.2.4: Each functional safety requirement shall be specified by considering the following, as applicable: a) operating modes; b — NON-COMPLIANT

Rationale: The document fails to provide any actual Functional Safety Requirements (FSRs) specifying operational context, time bounds, or redundancy mechanisms mandated by ISO 26262-3 Cl. 7.4.2.4.

Standard Expectation:

> *• Functional safety requirements must be derived from safety goals and explicitly address operating modes, fault-tolerant time intervals, safe states, emergency operation times, and functional redundancies where applicable.*

Analysis:

• No functional safety requirements are listed or detailed beyond the Safety Goals table; Cl. 7.4.2.4 mandates specification of these contextual elements per requirement.
• Evidence shows Safety Goals (SG-01 etc.) but lacks derivation into concrete FSRs addressing operating modes, FTTI implementation, safe states, emergency operations, or redundancies.
• The “Functional Safety Requirements” section ends abruptly without fulfilling Cl. 7.4.2.4’s mandatory sub-clauses (a–e).

Action Plan to Close Gap:
- Draft complete Functional Safety Requirements (FSRs) explicitly incorporating operating modes, FTTI, safe states, emergency operation time, and/or functional redundancies.
- Trace each FSR back to its originating safety goal via cross-reference or derivation matrix.

Evidence Reference: *File `Functional_Safety_Concept_LKA.pdf`, Page 1*

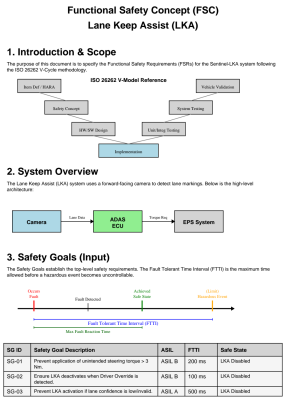


Fig ISO 26262-3 Cl. 7.4.2.4 - Evidence from Functional_Safety_Concept_LKA.pdf, Page 1

[ISO 26262-3 Cl. 7.4.2.8] ISO 26262-3 Cl. 7.4.2.8: The functional safety requirements shall be allocated to the elements of the system architectural design: a) During requ — NON-COMPLIANT

Rationale: Allocation of functional safety requirements to the system architectural design is absent despite presence of safety goals and conceptual documentation.

Standard Expectation:

> *• Functional safety requirements must be derived from safety goals and formally allocated to the system's architectural design per ISO 26262-3 Clause 7.4.2.8.*

Analysis:

• Evidence shows Safety Goals (SG-01 to SG-03) defined with ASIL levels and FTTI but lacks explicit derivation or linkage to system architecture.
• No architectural diagram, component mapping, or formal allocation matrix linking FSRs to hardware/software elements is provided.
• While "System Overview" mentions components like Camera → ECU → EPS, there is no documented assignment of safety requirements to these elements.

Action Plan to Close Gap:
- Create a system architectural design document showing mapped functional safety requirements assigned to each element (hardware/software).
- Include explicit derivations from safety goals to requirements using traceable links or matrices.
- Validate against ISO 26262-3 7.4.2.8 and ensure full coverage across all safety-critical functions.

Evidence Reference: *File `Functional_Safety_Concept_LKA.pdf`, Page 1*

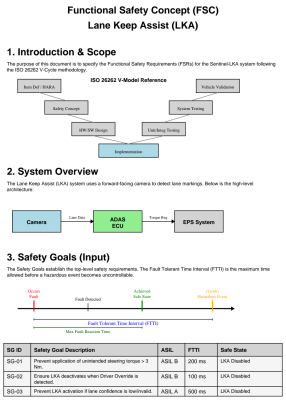


Fig ISO 26262-3 Cl. 7.4.2.8 - Evidence from Functional_Safety_Concept_LKA.pdf, Page 1

[ISO 26262-3 Cl. 7.4.2.9] ISO 26262-3 Cl. 7.4.2.9: If the functional safety concept relies on elements of other technologies, then the following shall apply: a) the functi — NON-COMPLIANT

Rationale: The documentation fails to demonstrate that safety requirements delegated to external technology components were properly specified and excluded from ASIL assignment.

Standard Expectation:

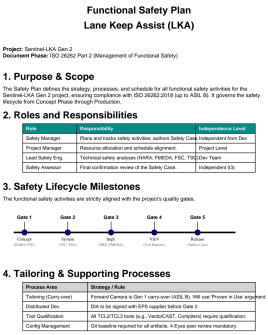
> *• When a functional safety concept relies on elements of other technologies, safety requirements related to those interfaces must be specified, their implementation verified via external means, and they must NOT carry an ASIL assignment.*

Analysis:

• No evidence shows delegation of safety requirements to external technologies (e.g., camera sensor, EPS actuator) or explicit exclusion of ASIL from them.
• While the FSC allocates responsibilities (“only elements inside dashed red line”), there’s no mention of interfacing with external tech or applying clause 7.4.2.9(d) regarding ASIL prohibition for outsourced safety functions.
• The Safety Goals table assigns ASIL levels (e.g., ASIL B) directly to safety objectives tied to hardware/software components like the ADAS ECU and camera—violating the rule that ASIL cannot be assigned to externally managed elements.

Action Plan to Close Gap:
- Identify all safety-critical interfaces with external technologies (camera, EPS, etc.) and formally decompose safety requirements away from internal system ownership.
- Explicitly annotate each delegated requirement with “No ASIL Assigned” per ISO 26262-3 7.4.2.9(c).
- Update the Functional Safety Concept to include a dedicated section detailing how external element safety attributes are validated per ISO 26262-4, including evidence references.

Evidence Reference: *File `Safety_Plan_LKA.pdf` , Page 1*



Functional Safety Plan
Lane Keep Assist (LKA)

Project: Sentinel-LKA Gen 2
Document Phase: ISO 26262 Part 2 (Management of Functional Safety)

1. Purpose & Scope

The Safety Plan defines the strategy, processes, and schedule for all functional safety activities for the Sentinel-LKA Gen 2 project, ensuring compliance with ISO 26262:2018 (up to ASIL B). It governs the safety lifecycle from Concept Phase through Production.

2. Roles and Responsibilities

Role	Responsibility	Independence Level
Safety Manager	Plans and tracks safety activities; authors Safety Case.	Independent from Dev
Project Manager	Resource allocation and schedule alignment.	Project Level
Lead Safety Eng.	Technical safety analyses (HARA, FMEDA, FSC, TSC).	Dev Team
Safety Assessor	Final confirmation review of the Safety Case.	Independent (I3)

3. Safety Lifecycle Milestones

The functional safety activities are strictly aligned with the project's quality gates.

Gate 1 Gate 2 Gate 3 Gate 4 Gate 5

4. Tailoring & Supporting Processes

Process Area	Strategy / Rule
Tailoring (Carry-over)	Forward Camera is Gen 1 carry-over (ASIL B). Will use 'Proven in Use' argument.
Distributed Dev.	DIA to be signed with EPS supplier before Gate 2.
Tool Qualification	All TCL3/TCL3 tools (e.g., VectorCAST, Complete) require qualification.
Config Management	Git baseline required for all artifacts. A Peer review mandatory.

Fig ISO 26262-3 Cl. 7.4.2.9 - Evidence from Safety_Plan_LKA.pdf, Page 1

[ISO 26262-3 Cl. 7.4.3] ISO 26262-3 Cl. 7.4.3: Safety validation criteria 7.4.3.1 The acceptance criteria for safety validation of the item shall be specified based on — NON-COMPLIANT

Rationale: Safety validation procedures, test cases, and pass/fail criteria are absent despite documented safety goals and lifecycle gates.

Standard Expectation:

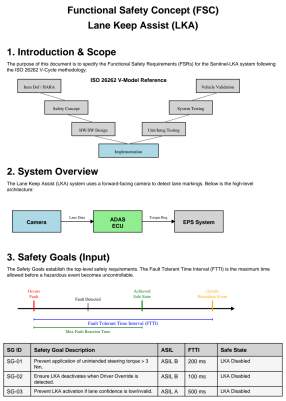
> *• Safety validation must be executed per plan using defined safety validation procedures, test cases, and pass/fail criteria tied to safety goals, functional safety requirements, and intended use, covering controllability, external measures, technology interactions, and assumption checks applicable only at vehicle level.*

Analysis:

• No safety validation procedures, test cases, or pass/fail criteria are referenced or presented in evidence for execution under ISO 26262-4 8.4.3.3(a).
• While safety goals (SG-01–SG-03) exist with ASIL, FTTI, and safe state definitions, no linkage to executable validation steps or acceptance criteria for safety validation is demonstrated.
• Evidence shows lifecycle gates but lacks documentation confirming safety validation planning or implementation against these goals.

Action Plan to Close Gap:
- Develop and attach formal safety validation procedures, test cases, and pass/fail criteria directly linked to each safety goal (SG-ID).
- Validate controllability, external measures, and assumption dependencies via vehicle-level test scenarios and confirm alignment with ISO 26262-4 8.4.3.2–8.4.3.4.

Evidence Reference: *File `Functional_Safety_Concept_LKA.pdf`, Page 1*



Functional Safety Concept (FSC)
Lane Keep Assist (LKA)

1. Introduction & Scope

The purpose of this document is to specify the Functional Safety Requirements (FSRs) for the Sentinel-LKA system following the ISO 26262 V-Cycle methodology.

ISO 26262 V-Model Reference

Item Def / HARA
Vehicle Validation
Safety Concept
System Testing
HW/SW Design
Unit/Integ Testing
Implementation

2. System Overview

The Lane Keep Assist (LKA) system uses a forward-facing camera to detect lane markings. Below is the high-level architecture:

Camera
Lane Data
ADAS ECU
Torque Req.
EPS System

3. Safety Goals (Input)

The Safety Goals establish the top-level safety requirements. The Fault Tolerant Time Interval (FTTI) is the maximum time allowed before a hazardous event becomes uncontrollable.

Occurs
Fault
Fault Detected
Achieved
Safe State
LLOAS
Hazardous Event
Fault Tolerant Time Interval (FTTI)
Max Fault Reaction Time

SG ID	Safety Goal Description	ASIL	FTTI	Safe State
SG-01	Prevent application of unintended steering torque > 3 Nm.	ASIL B	200 ms	LKA Disabled
SG-02	Ensure LKA deactivates when Driver Override is detected.	ASIL B	100 ms	LKA Disabled
SG-03	Prevent LKA activation if lane confidence is low/invalid.	ASIL A	500 ms	LKA Disabled

Fig ISO 26262-3 Cl. 7.4.3 - Evidence from Functional_Safety_Concept_LKA.pdf, Page 1

[ISO 26262-3 Cl. 7.4.4] ISO 26262-3 Cl. 7.4.4: Verification of the functional safety concept 7.4.4.1 The functional safety concept shall be verified in accordance with — NON-COMPLIANT

Rationale: The functional safety concept lacks explicit verification evidence against safety goals and mitigation capabilities as mandated by ISO 26262-8:2018 Clause 9.

Standard Expectation:

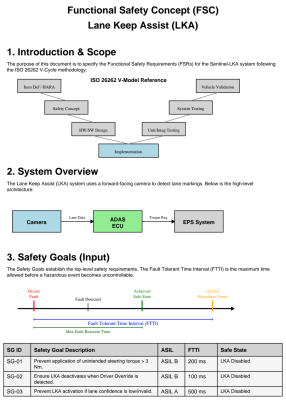
> *• The functional safety concept must be verified per ISO 26262-8:2018 Clause 9 to confirm consistency with safety goals and capability to mitigate/avoid hazards, using methods like testing, simulation, or expert judgment, with traceability via safety goals → requirements.*

Analysis:

• No verification report or method (per ISO 26262-8:2018 Clause 9) demonstrating how the FSC was validated against safety goals or hazard mitigation is provided.
• While Safety Goals (SG-01 etc.) exist and are decomposed into FSRs, there's no documented evidence of verification activity (tests, simulations, expert judgment) proving the FSC mitigates hazards or meets FTTI constraints.
• Traceability from goals to requirements exists (via decomposition), but absence of verification per Clause 9 renders the entire requirement non-compliant under 'Weakest Link'.

Action Plan to Close Gap:
- Develop and attach a formal Verification Report compliant with ISO 26262-8:2018 Clause 9, detailing how safety goals were confirmed via testing/simulation/expert evaluation.
- Include explicit documentation showing hazard mitigation effectiveness tied to each goal (e.g., FTTI adherence, safe state achievement timing).

Evidence Reference: *File `Functional_Safety_Concept_LKA.pdf`, Page 1*



Functional Safety Concept (FSC)
Lane Keep Assist (LKA)

1. Introduction & Scope

The purpose of this document is to specify the Functional Safety Requirements (FSRs) for the Sentinel-LKA system following the ISO 26262 V-Cycle methodology.

ISO 26262 V-Model Reference

Item Def / HARA
Safety Concept
HW/SW Design
Unit-level Testing
Implementation
Vehicle Validation
System Testing

2. System Overview

The Lane Keep Assist (LKA) system uses a forward-facing camera to detect lane markings. Below is the high-level architecture:

Camera
Lane Data
ADAS ECU
Torque Req.
EPS System

3. Safety Goals (Input)

The Safety Goals establish the top-level safety requirements. The Fault Tolerant Time Interval (FTTI) is the maximum time allowed before a hazardous event becomes uncontrollable.

Occurs
Fault
Fault Detected
Achieved
Safe State
(Latest
Hazardous Event
Fault Tolerant Time Interval (FTTI)
Max Fault Reaction Time

SG ID	Safety Goal Description	ASIL	FTTI	Safe State
SG-01	Prevent application of unintended steering torque > 3 Nm.	ASIL B	200 ms	LKA Disabled
SG-02	Ensure LKA deactivates when Driver Override is detected.	ASIL B	100 ms	LKA Disabled
SG-03	Prevent LKA activation if lane confidence is low/invalid.	ASIL A	500 ms	LKA Disabled

Fig ISO 26262-3 Cl. 7.4.4 - Evidence from Functional_Safety_Concept_LKA.pdf, Page 1

[ISO 26262-3 Cl. 7.4] ISO 26262-3 Cl. 7.4: Requirements and recommendations 7.4.1 General The functional safety requirements shall be specified in accordance with — NON-COMPLIANT

Rationale: Non-compliance stems from absence of documented derivation of functional safety requirements from safety goals and lack of explicit fault-handling strategies tied to FTTI and safe states.

Standard Expectation:

> *• Functional safety requirements must be derived from safety goals per ISO 26262-3 Clause 7.4.2, specifying fault-handling strategies including FTTI, safe states, and fault tolerance mechanisms, with direct traceability ensured across lifecycle phases.*

Analysis:

• Evidence shows Safety Goals table (SG-01–SG-03) but no functional safety requirements (FSRs) linked to them via derivation process.
• No explicit documentation of fault avoidance/detection, transition to safe state, or degradation strategy referenced against safety goals.
• Critical safety parameters like FTTI and safe state are mentioned contextually but not formally mapped into functional safety requirements.

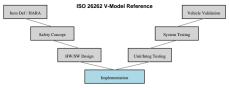
Action Plan to Close Gap:
- Develop and attach formal functional safety requirements (FSRs) directly derived from each safety goal listed in the Safety Goals table.
- Explicitly link each FSR to its originating safety goal(s) using traceability matrices or cross-references.
- Define and include mandatory fault-handling strategies (fault detection, safe state transitions, degradation paths) within FSRs based on ASIL and FTTI values.

Evidence Reference: *File `Functional_Safety_Concept_LKA.pdf`, Page 1*

Functional Safety Concept (FSC)
Lane Keep Assist (LKA)

1. Introduction & Scope

The purpose of this document is to specify the Functional Safety Requirements (FSRs) for the Sentinel-LKA system following the ISO 26262 V-Cycle methodology.



2. System Overview

The Lane Keep Assist (LKA) system uses a forward-facing camera to detect lane markings. Below is the high-level architecture.

3. Safety Goals (Input)

The Safety Goals establish the top-level safety requirements. The Fault Tolerant Time Interval (FTTI) is the maximum time allowed before a hazardous event becomes uncontrollable.

SG ID	Safety Goal Description	ASIL	FTTI	Safe State
SG-01	Prevent application of unintended steering torque > 3 Nm.	ASIL B	200 ms	LKA Disabled
SG-02	Ensure LKA deactivates when Driver Override is detected.	ASIL B	100 ms	LKA Disabled
SG-03	Prevent LKA activation if lane confidence is low/invalid.	ASIL A	500 ms	LKA Disabled

Fig ISO 26262-3 Cl. 7.4 - Evidence from Functional_Safety_Concept_LKA.pdf, Page 1