

Technical Safety Concept Lane Assistance

**Document Version: 1.1**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 11.03.2018 | 1.0 | Nathan Greco | First Draft |
| 18.03.2018 | 1.1 | Nathan Greco | Updated for second submission |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Table of Contents

[Document history](#_1t3h5sf)

[Table of Contents](#_ktt3lgighckp)

[Purpose of the Technical Safety Concept](#_fulgh8sf1ocg)

[Inputs to the Technical Safety Concept](#_757cx6xm46zb)

[Functional Safety Requirements](#_2f9rjqxbsp2)

[Refined System Architecture from Functional Safety Concept](#_qp3s9pvua9mt)

[Functional overview of architecture elements](#_cqb49updinx4)

[Technical Safety Concept](#_mx8us8onanqo)

[Technical Safety Requirements](#_lnxjuovv6kca)

[Refinement of the System Architecture](#_74udkdvf7nod)

[Allocation of Technical Safety Requirements to Architecture Elements](#_g2lqf7kmbspk)

[Warning and Degradation Concept](#_4w6r8buy4lrp)

# Purpose of the Technical Safety Concept

The technical safety concept is a component level plan that defines both the architecture being implemented and the safety goals necessary to ensure the system satisfies ISO 26262.

# Inputs to the Technical Safety Concept

## Functional Safety Requirements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  01-01 | The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude | C | 50 ms | LDW Disabled with visual indication |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency. | C | 50 ms | LDW Disabled with visual indication |
| Functional  Safety  Requirement  01-03 | As soon as the LDW function fails to detect the lane lines, the ‘LDW Safety' software block shall disable the system and send a signal to the car display ECU to turn on a warning light. | B | 50 ms | LDW Disabled with visual indication |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only ‘Max\_Duration’. | B | 500 ms | LDW Disabled with visual indication |
| Functional  Safety  Requirement  02-02 | As soon as the LKA function fails to detect the lane lines, the ‘LKA Safety' software block shall disable the system and send a signal to the car display ECU to turn on a warning light. | B | 50 ms | LKA Disabled with visual indication |

## Refined System Architecture from Functional Safety Concept

## 

**Figure 1** – Detailed system architecture with ASIL ratings

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Camera device that retrieves images of the road in front of the vehicle |
| Camera Sensor ECU - Lane Sensing | Process within ECU which processes image from the camera sensor with computer vision algorithms to determine the vehicles relative position to the lane, used by both LDW and LKA systems |
| Camera Sensor ECU - Torque request generator | Process within ECU which generates the torque to be commands for the motor |
| Car Display | An informative display to display the road lines and their orientation, display warning and alert messages, and is the primary GUI for the vehicle operator |
| Car Display ECU - Lane Assistance On/Off Status | Process within the ECU which determines the lane assist system’s on/off status |
| Car Display ECU - Lane Assistant Active/Inactive | Process within the ECU which determines the lane assist system’s active statys |
| Car Display ECU - Lane Assistance malfunction warning | Process within the ECU which monitors the health of the LKA system and alerts the driver to faults in the system |
| Driver Steering Torque Sensor | A sensor that measures that amount of effort the driver is making to steer the vehicle. This is important so that we do not interfere with intentional steering commands from the driver and impede his ability to control the vehicle |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Process with handles torque requests and drives the command of the motor |
| EPS ECU - Normal Lane Assistance Functionality | Process within the EPS ECU that manages the overall modes and state machine of the system |
| EPS ECU - Lane Departure Warning Safety Functionality | Process within the EPS ECU that checks the health of the LDW system and triggers any necessary safety modes |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Process within the EPS ECU that checks the health of the LKA system and triggers any necessary safety modes |
| EPS ECU - Final Torque | Process within the EPS ECU that generates the final torque command |
| Motor | The actuator that directly influences the steering of the vehicle. It receives its command from the power steering ECU |

# Technical Safety Concept

## Technical Safety Requirements

**Lane Departure Warning (LDW) Requirements:**

Functional Safety Requirement 01-01 with its associated system elements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  01-01 | The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude | **X** |  |  |

Technical Safety Requirements related to Functional Safety Requirement 01-01 are:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Architecture Allocation** | **Safe State** |
| Technical  Safety  Requirement  01 | The LDW safety component shall ensure that the amplitude of the 'LDW\_Torque\_Request' sent to the 'Final electronic power steering Torque' component is below 'Max\_Torque\_Amplitude. | C | 50 ms | LDW Safety | LDW Disabled and torque set to 0 |
| Technical  Safety  Requirement  02 | As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light. | C | 50 ms | LDW Safety | LDW Disabled and torque set to 0 |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW\_Torque\_Request' shall be set to zero. | C | 50 ms | LDW Safety | LDW Disabled and torque set to 0 |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured. | C | 50 ms | LDW Safety | LDW Disabled and torque set to 0 |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | A | Ignition Cycle | LDW Safety | LDW Disabled and torque set to 0 |

Functional Safety Requirement 01-02 with its associated system elements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency. | **X** |  |  |

Technical Safety Requirements related to Functional Safety Requirement 01-02 are:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Architecture Allocation** | **Safe State** |
| Technical  Safety  Requirement  06 | The LDW safety component shall ensure that the frequency of the 'LDW\_Torque\_Request' sent to the 'Final electronic power steering Torque' component is below 'Max\_Torque\_Frequency. | C | 50 ms | LDW Safety | LDW Disabled and torque set to 0 |

Functional Safety Requirement 01-03 with its associated system elements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  01-03 | As soon as the LDW function fails to detect the lane lines, the ‘LDW Safety' software block shall disable the system and send a signal to the car display ECU to turn on a warning light. | **X** |  | **X** |

Technical Safety Requirements related to Functional Safety Requirement 01-03 are:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  07 | The LDW safety component must detect a failure to detect lane lines in the road and create a fault condition. | B | 50 ms | LDW Safety | LDW Disabled and torque set to 0 with visual indication |

**Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:**

|  |  |  |
| --- | --- | --- |
| **ID** | **Validation Acceptance**  **Criteria and Method** | **Verification Acceptance**  **Criteria and Method** |
| Technical  Safety  Requirement  01 | Perform a study to determine minimum noticeable magnitude torque commands for a driver to notice the alter and maximum for the driver to maintain control of the vehicle. | Impose these limits and attempt to create commands outside these limits to verify the actuator does not actuate at these values. |
| Technical  Safety  Requirement  02 | Determine scenarios where disabling of the system is an appropriate response | Verify that anytime system is disabled, output torque is set to 0 and an indicator light is turned on. |
| Technical  Safety  Requirement  03 | Tests should be done to determine pass/fail criteria for confidence in the lane detection algorithm. | If confidence in the lane detection is below the pass/fail criteria, the system should deactivate and alert driver. |
| Technical  Safety  Requirement  04 | A tolerance window for 'LDW\_Torque\_Request' should be determined that keeps control stable | The actual command commanded torque should never deviate outside of that window of 'LDW\_Torque\_Request' |
| Technical  Safety  Requirement  05 | Zero memory defects of any kind should be tolerated | Any memory defects found should disable lane keep system |
| Technical  Safety  Requirement  06 | Perform a study to determine minimum noticeable frequency torque commands for a driver to notice the alter and maximum for the driver to maintain control of the vehicle | Impose these limits and attempt to create commands outside these limits to verify the actuator does not actuate at these values |
| Technical  Safety  Requirement  07 | Evaluate frequency and duration of interruptions to the lane detection status and determine a time delay that would not pickup false positives | Operate the vehicle and blind the camera so road lanes are not detected. Verify that the vehicle alerts the driver within the identified time window |

**Lane Keeping Assistance (LKA) Requirements:**

Functional Safety Requirement 02-01 with its associated system elements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **D** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only ‘Max\_Duration’. | **X** |  |  |

Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  08 | The LKA safety component shall limit the duration of applied torque to ‘Max\_Duration’. | B | 500 ms | LKA Safety | LKA Disabled and torque set to 0 |
| Technical  Safety  Requirement  09 | As soon as the LKA function deactivates the LKA feature, the 'LKA Safety' software block shall send a signal to the car display ECU to turn on a warning light. | B | 500 ms | LKA Safety | LKA Disabled and torque set to 0 |
| Technical  Safety  Requirement  10 | As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the 'LKA\_Torque\_Request' shall be set to zero. | B | 500 ms | LKA Safety | LKA Disabled and torque set to 0 |
| Technical  Safety  Requirement  11 | The validity and integrity of the data transmission for 'LKA\_Torque\_Request' signal shall be ensured. | B | 500 ms | LKA Safety | LKA Disabled and torque set to 0 |
| Technical  Safety  Requirement  12 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | A | Ignition Cycle | LDW Safety | LKA Disabled and torque set to 0 |

Functional Safety Requirement 02-02 with its associated system elements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  02-02 | As soon as the LKA function fails to detect the lane lines, the ‘LKA Safety' software block shall disable the system and send a signal to the car display ECU to turn on a warning light. | **X** |  | **X** |

Technical Safety Requirements related to Functional Safety Requirement 02-02 are:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  13 | The LKA safety component must detect a failure to detect lane lines in the road and create a fault condition. | B | 50 ms | LKA Safety | LKA Disabled with visual indication |

**Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:**

|  |  |  |
| --- | --- | --- |
| **ID** | **Validation Acceptance**  **Criteria and Method** | **Verification Acceptance**  **Criteria and Method** |
| Technical  Safety  Requirement  08 | Perform a study to determine the maximum permissible time that somebody using the system properly may allow the system to adjust | Verify if the system exceeds that duration in time the system is disabled. |
| Technical  Safety  Requirement  09 | Determine scenarios where disabling of the system is an appropriate response | Verify that anytime system is disabled, output torque is set to 0 and an indicator light is turned on. |
| Technical  Safety  Requirement  10 | Tests should be done to determine pass/fail criteria for confidence in the lane detection algorithm. | If confidence in the lane detection is below the pass/fail criteria, the system should deactivate and alert driver. |
| Technical  Safety  Requirement  11 | A tolerance window for 'LDW\_Torque\_Request' should be determined that keeps control stable | The actual command commanded torque should never deviate outside of that window of 'LDW\_Torque\_Request' |
| Technical  Safety  Requirement  12 | Zero memory defects of any kind should be tolerated | Any memory defects found should disable lane keep system |
| Technical  Safety  Requirement  13 | Evaluate frequency and duration of interruptions to the lane detection status and determine a time delay that would not pickup false positives | Operate the vehicle and blind the camera so road lanes are not detected. Verify that the vehicle alerts the driver within the identified time window |

## Refinement of the System Architecture

## https://d17h27t6h515a5.cloudfront.net/topher/2017/July/59783620_refined-system-architecture-01/refined-system-architecture-01.png

**Figure 2** – Detailed system architecture with ASIL ratings

## Allocation of Technical Safety Requirements to Architecture Elements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Technical  Safety  Requirement  01 | The LDW safety component shall ensure that the amplitude of the 'LDW\_Torque\_Request' sent to the 'Final electronic power steering Torque' component is below 'Max\_Torque\_Amplitude. | **X** |  |  |
| Technical  Safety  Requirement  02 | As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light. | **X** |  |  |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW\_Torque\_Request' shall be set to zero. | **X** |  |  |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured. | **X** |  |  |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | **X** |  |  |
| Technical  Safety  Requirement  06 | The LDW safety component shall ensure that the frequency of the 'LDW\_Torque\_Request' sent to the 'Final electronic power steering Torque' component is below 'Max\_Torque\_Frequency. | **X** |  |  |
| Technical  Safety  Requirement  07 | The LDW safety component must detect a failure to detect lane lines in the road and create a fault condition. | **X** |  | **X** |
| Technical  Safety  Requirement  08 | The LKA safety component shall limit the duration of applied torque to ‘Max\_Duration’. | **X** |  |  |
| Technical  Safety  Requirement  09 | As soon as the LKA function deactivates the LKA feature, the 'LKA Safety' software block shall send a signal to the car display ECU to turn on a warning light. | **X** |  |  |
| Technical  Safety  Requirement  10 | As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the 'LKA\_Torque\_Request' shall be set to zero. | **X** |  |  |
| Technical  Safety  Requirement  11 | The validity and integrity of the data transmission for 'LKA\_Torque\_Request' signal shall be ensured. | **X** |  |  |
| Technical  Safety  Requirement  12 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | **X** |  |  |
| Technical  Safety  Requirement  13 | The LKA safety component must detect a failure to detect lane lines in the road and create a fault condition. | **X** |  | **X** |

## 

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Disable LDW and alert | Malfunction\_01 | Yes | Driver indication of fault in LDW system |
| WDC-02 | Disable LDW and alert | Malfunction\_02 | Yes | Driver indication of fault in LDW system |
| WDC-03 | Disable LKA and alert | Malfunction\_03 | Yes | Driver indication of fault in LKA system |
| WDC-04 | Disable LDW and alert | Malfunction\_04 | Yes | Driver indication of fault in LDW system |
| WDC-05 | Disable LKA and alert | Malfunction\_05 | Yes | Driver indication of fault in LKA system |