

Technical Safety Concept Lane Assistance

**Document Version: 1.0**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 06/04/2019 | 1.0 | Jian Li | Initial version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Table of Contents

[Document history](#_Toc735908384)

[Table of Contents](#_Toc1053886815)

[Purpose of the Technical Safety Concept](#_Toc230579249)

[Inputs to the Technical Safety Concept](#_Toc1284938755)

[Functional Safety Requirements](#_Toc870101053)

[Refined System Architecture from Functional Safety Concept](#_Toc1572245348)

[Functional overview of architecture elements](#_Toc2088771148)

[Technical Safety Concept](#_Toc1061506927)

[Technical Safety Requirements](#_Toc1600266460)

[Refinement of the System Architecture](#_Toc593198192)

[Allocation of Technical Safety Requirements to Architecture Elements](#_Toc1262923570)

[Warning and Degradation Concept](#_Toc228074042)

# Purpose of the Technical Safety Concept

# 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 | 50ms | Turn off LDW |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency. | C | 50ms | Turn off LDW |
| 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 | 500ms | Turn off LKA |

## Refined System Architecture from Functional Safety Concept



### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | The Camera Sensor reads the images from the road. |
| Camera Sensor ECU - Lane Sensing | Identifies the lane. |
| Camera Sensor ECU - Torque request generator | Sends the appropriate messages to electronic power steering ECU about steering wheel torque. |
| Car Display | Shows the function to the driver. |
| Car Display ECU - Lane Assistance On/Off Status | Controls to show Lane Assistance On/Off Status on the display. |
| Car Display ECU - Lane Assistant Active/Inactive | Controls to show Lane Assistant Active/Inactive on the display. |
| Car Display ECU - Lane Assistance malfunction warning | Controls to show Lane Assistance malfunction warning on the display. |
| Driver Steering Torque Sensor | Measures the torque value of the steering wheel. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Handles the driver torque steering torque. |
| EPS ECU - Normal Lane Assistance Functionality | Sends the vibration torque request. |
| EPS ECU - Lane Departure Warning Safety Functionality | Receives the vibration torque request from the basic lane keeping functionality block, and checks to make sure that the torque request is below the maximum amplitude and frequency and sends its torque request to the final EPS torque generator block, and also a status signal to the car display. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Ensures that the lane keeping assistance torque is applied for only Max\_Duration. |
| EPS ECU - Final Torque | Determine the final torque value that is applied to the steering wheel. |
| Motor | Applies force to the steering wheel under the control of final torque. |

# Technical Safety Concept

## Technical Safety Requirements

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

Functional Safety Requirement 01-01 with its associated system elements

(derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 | 50ms | LDW Safety | LDW torque output is set to zero. |
| Technical  Safety  Requirement  02 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured. | C | 50ms | Data Transmission Integrity Check | N/A |
| 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 | 50ms | LDW Safety | LDW torque output is set to zero. |
| Technical  Safety  Requirement  04 | 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 | 50ms | LDW Safety | LDW torque output is set to zero. |
| 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 | Memory Test | LDW torque output is set to zero. |

Functional Safety Requirement 01-2 with its associated system elements

(derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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  01 | 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 | 50ms | LDW Safety | LDW torque output is set to zero. |
| Technical  Safety  Requirement  02 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured. | C | 50ms | Data Transmission Integrity Check | N/A |
| 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 | 50ms | LDW Safety | LDW torque output is set to zero. |
| Technical  Safety  Requirement  04 | 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 | 50ms | LDW Safety | LDW torque output is set to zero. |
| 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 | Memory Test | LDW torque output is set to zero. |

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

**[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]**

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

Functional Safety Requirement 02-1 with its associated system elements

(derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  02-01 | The lane keeping item 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  01 | The LKA safety component shall ensure that the active time shall below ‘Max\_Duration’. | B | 500ms | LKA Safety | LKA torque output is set to zero. |
| Technical  Safety  Requirement  02 | The validity and integrity of the data transmission for 'LKA\_Torque\_Request' signal shall be ensured. | B | 500ms | Data Transmission Integrity Check | N/A |
| Technical  Safety  Requirement  03 | 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 | 500ms | LKA Safety | LKA torque output is set to zero. |
| Technical  Safety  Requirement  04 | 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 | 500ms | LKA Safety | LKA torque output is set to zero. |
| 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 | Memory Test | LKA torque output is set to zero. |

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

**[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]**

## Refinement of the System Architecture

****

## Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements are allocated to the Electronic Power Steering ECU.

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off the function | Torque crosses the Max\_Torque | Yes | The warning light is on. |
| WDC-02 | Turn off the function | Activated time elapsed over Max\_Duration | Yes | The warning light is on. |