

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

**Template Version 1.0, Released on 2017-06-21**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2017/08/13 | 1.0 | Yuesong Xie | First Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Table of Contents

Contents

[Document history 2](#_Toc490397761)

[Table of Contents 2](#_Toc490397762)

[Purpose of the Technical Safety Concept 2](#_Toc490397763)

[Inputs to the Technical Safety Concept 3](#_Toc490397764)

[Functional Safety Requirements 3](#_Toc490397765)

[Refined System Architecture from Functional Safety Concept 3](#_Toc490397766)

[Functional overview of architecture elements 4](#_Toc490397767)

[Technical Safety Concept 5](#_Toc490397768)

[Technical Safety Requirements 5](#_Toc490397769)

[Refinement of the System Architecture 9](#_Toc490397770)

[Allocation of Technical Safety Requirements to Architecture Elements 10](#_Toc490397771)

[Warning and Degradation Concept 10](#_Toc490397772)

# Purpose of the Technical Safety Concept

Refines the functional safety concept and allocates technical safety requirements to hardware and software components

# 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 electronic power steering ECU shall ensure that the oscillating torque amplitude is below Max\_Torque\_Amplitude | C | 50ms | Off |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the oscillating torque frequency is below Max\_Torque\_Frequency | C | 50ms | Off |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max\_Duration | C | 50ms | Off |

## Refined System Architecture from Functional Safety Concept

### C:\Users\Yuesong Xie\AppData\Local\Microsoft\Windows\INetCache\Content.Word\graphic_asset_4.png

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Sends an image stream to the Camera Sensor ECU |
| Camera Sensor ECU - Lane Sensing | Responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake |
| Camera Sensor ECU - Torque request generator | Sends torque request to Lane Assistance functionality |
| Car Display | Provides feedback to the driver about on/off, active/inactive and malfunction status of the Lane Assistance system |
| Car Display ECU - Lane Assistance On/Off Status | Provides feedback to the driver about on/off status of the Lane Assistance system |
| Car Display ECU - Lane Assistant Active/Inactive | Provides feedback to the driver about active/inactive status of the Lane Assistance system |
| Car Display ECU - Lane Assistance malfunction warning | Provides feedback to the driver about malfunction status of the Lane Assistance system. Receives input from LDW Safety Functionality (LDW\_Error\_Status) |
| Driver Steering Torque Sensor | Responsible for measuring the torque provided by the driver |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Responsible for processing input from the Driver Steering Torque Sensor and sending output to the EPS ECU - Final Torque |
| EPS ECU - Normal Lane Assistance Functionality | Responsible for processing the input from the Camera Sensor ECU and sending Primary\_LDW\_Torque\_Request to the LA Safety Functionality |
| EPS ECU - Lane Departure Warning Safety Functionality | Part of the Lane Keeping Assistant Safety Functionality. Processes input from Safety Startup and Data Transmission Integrity Check. Sends LDW\_Torque\_Request and LDW\_Activation\_Status to Final Torque. Sends LDW\_Error\_Status to LA Malfunction Warning in the Car Display ECU |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Processes Primary\_LDW\_Torque\_Request from the Normal Lane Assistance Functionality |
| EPS ECU - Final Torque | Processes all steering torque related inputs and sends a final torque request to the Motor |
| Motor | Carries out the Electronic Power Steering ECU torque request and provides torque to the steering wheel |

# 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 Functionality | Off |
| 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 | 50ms | LDW Safety Functionality | Off |
| 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 Functionality | Off |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured | C | 50ms | Data Transmission Integrity Check | Off |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory | A | Ignition cycle | Safety Startup | Off |

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 Functionality | Off |
| 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 | 50ms | LDW Safety Functionality | Off |
| 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 Functionality | Off |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured | C | 50ms | Data Transmission Integrity Check | Off |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | Ignition cycle | Safety Startup | Off |

**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 LDW safety component shall ensure that the 'LDW\_Torque\_Request' sent to the 'Final electronic power steering Torque' component is applied for only Max\_Duration | B | 500ms | LDW Safety Functionality | Off |
| 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 | B | 50ms | LDW Safety Functionality | Off |
| 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. | B | 50ms | LDW Safety Functionality | Off |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured | B | 50ms | Data Transmission Integrity Check | Off |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | Ignition cycle | Safety Startup | Off |

**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

**[Instructions: Include the refined system architecture. Hint: The refined system architecture should include the system architecture from the end of the technical safety lesson, including all of the ASIL labels.]**

## Allocation of Technical Safety Requirements to Architecture Elements

For the Lane Keeping item, 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 | Off | Oscillating torque frequency is above Max\_Torque\_Amplitude or Max\_Torque\_Frequency | Yes | LED on Car Display |
| WDC-01 | Off | Lane keeping assistance torque is applied for more than Max\_Duration | Yes | LED on Car Display |