

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| June 21, 2017 | 1.0 | Udacity, EB | Template version |
| April 23, 2019 | 1.1 | Ahmed Belal | Finalize the document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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 purpose of the technical safety concept (TSC) is to get into more details of the functional safety concept (FSC) including:

* Turning functional safety requirements into technical safety requirements
* Allocating the technical safety requirements to the system architecture

# 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 (EPS) ECU shall ensure that the lane departure oscillating torque amplitude is below the MAX\_TORQUE\_AMPLITUDE | C | 50ms | Shut the system down by setting lane assistance output is set to zero |
| Functional  Safety  Requirement  01-02 | The electronic power steering (EPS) ECU shall ensure that the lane departure oscillating torque frequency is below the MAX\_TORQUE\_FREQUENCY | C | 50ms | Shut the system down by setting lane assistance output is set to zero |
| Functional  Safety  Requirement  02-01 | The electronic power steering (EPS) ECU shall ensure that the lane keeping assistance (LKA) torque is applied for only MAX\_DURATION | B | 50ms | Shut the system down by setting lane assistance output is set to zero |
| Functional  Safety  Requirement  03-01 | The electronic power steering (EPS) ECU shall ensure that the lane keeping assistance (LKA) torque is below the MAX\_TORQUE\_AMPLITUDE when active in order to stay in ego lane | C | 50ms | Shut the system down by setting lane assistance output is set to zero |
| Functional  Safety  Requirement  04-01 | The electronic power steering (EPS) ECU shall ensure that the lane keeping assistance (LKA) torque is applied in the correct direction when active in order to stay in ego lane | C | 50ms | Shut the system down by setting lane assistance output is set to zero |

## Refined System Architecture from Functional Safety Concept



### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Capture the road images (video) |
| Camera Sensor ECU - Lane Sensing | Processing the images (video) provided by the camera sensor for detecting the lane lines |
| Camera Sensor ECU - Torque request generator | determines when the vehicle leaves the lane by mistake, and calculate/send the appropriate torque request to the electronic power steering (EPS) ECU |
| Car Display | Screen for showing the notification, warnings and vehicle status for the driver |
| Car Display ECU - Lane Assistance On/Off Status | Shows on Car display an indicator for Lane Assistant Active/Inactive |
| Car Display ECU - Lane Assistant Active/Inactive | Shows on Car display an indicator for Lane Assistance On/Off Status |
| Car Display ECU - Lane Assistance malfunction warning | Shows on Car display an indicator for Lane Assistance malfunction warning |
| Driver Steering Torque Sensor | Measure the steering torque applied on the steering wheels |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Receives the measured steering torque by the driving steering torque sensor |
| EPS ECU - Normal Lane Assistance Functionality | Responsible for the normal functionality for the lane assistance features including receiving the camera images and calculating the primary LKA/LDW torque request |
| EPS ECU - Lane Departure Warning Safety Functionality | The functional safety module that ensures that LDW primary torque amplitude and frequency is below the specified limit, otherwise it will go to the specified safe state |
| EPS ECU - Lane Keeping Assistant Safety Functionality | The functional safety module that ensures that LKA primary torque amplitude is applied gradually, below the specified limit, and applied in the correct direction, otherwise it will go to the specified safe state |
| EPS ECU - Final Torque | Sends the final LKA/LDW torque request to the motor to be applied on the steering wheel |
| Motor | Apply the steering torque based on the received steering control signal from the Electronic power steering (EPS) ECU |

# 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 electronic power steering (EPS) ECU shall ensure that the lane departure oscillating torque amplitude is below the MAX\_TORQUE\_AMPLITUDE | ✔ |  |  |

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 lane departure warning (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 block | Shut down the LDW system by setting ‘LDW\_Torque\_Request’ to zero |
| Technical  Safety  Requirement  02 | The validity and integrity of data transmission for ‘LDW\_Torque\_Request’ signal shall be ensured | C | 50ms | Data Transmission Integrity Check | Shut down the LDW system by setting ‘LDW\_Torque\_Request’ to zero |
| Technical  Safety  Requirement  03 | As soon as failure detected by lane departure warning (LDW) function, it shall deactivate the LDW feature and the ‘LDW\_Torque\_Request’ shall set to zero | C | 50ms | LDW Safety block | Shut down the LDW system by setting ‘LDW\_Torque\_Request’ to zero |
| Technical  Safety  Requirement  04 | As soon as the LDW function deactivate 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 block | Shut down the LDW system by setting ‘LDW\_Torque\_Request’ to zero |
| Technical  Safety  Requirement  05 | Memory tests shall be conducted at startup of the EPS ECU to check for any faults in memory | A | Length of the vehicle ignition cycle | Memory Tests Check | Restart the LDW system, if this repeated for 3 times, display error signal on the car display |

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 electronic power steering (EPS) ECU shall ensure that the lane departure oscillating torque frequency is below MAX\_TORQUE\_FREQUENCY | ✔ |  |  |

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 lane departure warning (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 block | Shut down the LDW system by setting ‘LDW\_Torque\_Request’ to zero |
| Technical  Safety  Requirement  02 | The validity and integrity of data transmission for ‘LDW\_Torque\_Request’ signal shall be ensured | C | 50ms | Data Transmission Integrity Check | Shut down the LDW system by setting ‘LDW\_Torque\_Request’ to zero |
| Technical  Safety  Requirement  03 | As soon as failure detected by lane departure warning (LDW) function, it shall deactivate the LDW feature and the ‘LDW\_Torque\_Request’ shall set to zero | C | 50ms | LDW Safety block | Shut down the LDW system by setting ‘LDW\_Torque\_Request’ to zero |
| Technical  Safety  Requirement  04 | As soon as the LDW function deactivate 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 block | Shut down the LDW system by setting ‘LDW\_Torque\_Request’ to zero |
| Technical  Safety  Requirement  05 | Memory tests shall be conducted at startup of the EPS ECU to check for any faults in memory | A | Length of the vehicle ignition cycle | Memory Tests Check | Restart the LDW system, if this repeated for 3 times, display error signal on the car display |

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

Verification and validation are identified for each technical safety requirement (TSR).

“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.

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria as the same as Functional Safety Concept.

|  |  |  |
| --- | --- | --- |
| **ID** | **Validation Acceptance**  **Criteria and Method** | **Verification Acceptance**  **Criteria and Method** |
| Technical  Safety  Requirement  01 | Validate the LDW MAX\_TORQUE\_AMPLITUDE of the oscillating steering torque | Verify that the LDW will shut down if the MAX\_TORQUE\_AMPLITUDE exceeded |
| Technical  Safety  Requirement  02 | Validate the LDW MAX\_TORQUE\_FREQUENCY of the oscillating steering torque | Verify that the LDW will shut down if the MAX\_TORQUE\_ FREQUENCY exceeded |

**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 electronic power steering (EPS) ECU shall ensure that the lane keeping assistance (LKA) torque is applied for only MAX\_DURATION time duration | ✔ |  |  |

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 | Lane Keeping Assistance (LKA) safety component shall ensure that the torque of the ‘LKA\_Torque\_Request’ sent to the ‘final electronic power steering torque’ component is applied for only MAX\_DURATION time duration | C | 500ms | LKA Safety block | Shut down the LDW system by setting ‘LKA\_Torque\_Request’ to zero |
| Technical  Safety  Requirement  02 | The validity and integrity of data transmission for ‘LKA\_Torque\_Request’ signal shall be ensured | C | 500ms | Data Transmission Integrity Check | Shut down the LDW system by setting ‘LKA\_Torque\_Request’ to zero |
| Technical  Safety  Requirement  03 | As soon as failure detected by Lane Keeping Assistance (LKA) function, it shall deactivate the LKA feature and the ‘LKA\_Torque\_Request’ shall set to zero | C | 500ms | LKA Safety block | Shut down the LDW system by setting ‘LKA\_Torque\_Request’ to zero |
| Technical  Safety  Requirement  04 | As soon as the LKA function deactivate the LKA feature, the ‘LKA Safety’ software block shall send a signal to the car display ECU to turn on a warning light | C | 500ms | LKA Safety block | Shut down the LDW system by setting ‘LKA\_Torque\_Request’ to zero |
| Technical  Safety  Requirement  05 | Memory tests shall be conducted at startup of the EPS ECU to check for any faults in memory | A | Length of the vehicle ignition cycle | Memory Tests Check | Restart the LKA system, if this repeated for 3 times, display error signal on the car display |

Functional Safety Requirement 03-1 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  03-01 | The electronic power steering (EPS) ECU shall ensure that the lane keeping assistance (LKA) torque is below the MAX\_TORQUE\_AMPLITUDE when active in order to stay in ego lane | ✔ |  |  |

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  01 | Lane Keeping Assistance (LKA) safety component shall ensure that the amplitude of the ‘LKW\_Torque\_Request’ sent to the ‘final electronic power steering torque’ component is below MAX\_TORQUE\_AMPLITUDE | C | 500ms | LKA Safety block | Shut down the LDW system by setting ‘LKA\_Torque\_Request’ to zero |

Functional Safety Requirement 04-1 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  03-01 | The electronic power steering (EPS) ECU shall ensure that the lane keeping assistance (LKA) torque is applied in the correct direction when active in order to stay in ego lane | ✔ |  |  |

Technical Safety Requirements related to Functional Safety Requirement 04-01 are:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  01 | Lane Keeping Assistance (LKA) safety component shall ensure that the torque of the ‘LKW\_Torque\_Request’ sent to the ‘final electronic power steering torque’ component is applied in the correct direction when active in order to stay in ego lane | C | 500ms | LKA Safety block | Shut down the LDW system by setting ‘LKA\_Torque\_Request’ to zero |

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

Verification and validation are identified for each technical safety requirement (TSR).

“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.

Lane Keeping Assistance (LKA)Verification and Validation Acceptance Criteria as the same as Functional Safety Concept.

|  |  |  |
| --- | --- | --- |
| **ID** | **Validation Acceptance**  **Criteria and Method** | **Verification Acceptance**  **Criteria and Method** |
| Technical  Safety  Requirement  02-01 | Validate the LKA MAX\_DURATION of the steering torque | Verify that the LKA will shut down if the steering torque MAX\_DURATION exceeded |
| Technical  Safety  Requirement  03-01 | Validate the LKA MAX\_TORQUE\_AMPLITUDE of the steering torque | Verify that the LKA will shut down if the MAX\_TORQUE\_AMPLITUDE exceeded |
| Technical  Safety  Requirement  04-01 | Validate the LKA correct steering torque direction | Verify that the LKA will shut down if the steering torque applied in the wrong direction |

## Refinement of the System Architecture



## Allocation of Technical Safety Requirements to Architecture Elements

Technical safety requirements already allocated to the architecture elements in the technical safety requirements tables. Generally, all technical safety requirements are allocated to the electronic power steering (EPS) ECU.

## Warning and Degradation Concept

We've already identified that for any system malfunction, the lane assistance functions will be turned off and the driver will receive a warning light indication. The technical safety requirements have not changed how functionality will be degraded or what the warning will be.

So in this case, the warning and degradation concept is the same for the technical safety requirements as for the functional safety requirements**.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Shut the system down by setting lane assistance output is set to zero | Malfunction\_01  Malfunction\_02 | Yes | Display LDW warning on driver dashboard |
| WDC-02 | Shut the system down by setting lane assistance output is set to zero | Malfunction\_03  Malfunction\_04  Malfunction\_05 | Yes | Display LKA warning on driver dashboard |

For more information about the list of malfunctions, please check the Functional safety concept (FSC) document page 5.