

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 01/10/2018 | 1.0 | Anil Kumar | First version of 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 technical safety concept involves:

* Turning functional safety requirements into technical safety requirements
* Defining other into technical safety requirements for :
  + Detecting Faults within a system
  + Detecting faults in an external device interacting with the system
  + Reaching the safe state
  + Implementing a warning and degradation concept
  + Preventing latent faults
* Allocating technical safety requirements to the system architecture
* Defining attributes to the requirements

# 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 oscillation torque amplitude is below Max\_Torque\_Amplitude | C | 50ms | The oscillation torque amplitude is below Max\_Torque\_Amplitude |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillation torque frequency is below Max\_Torque\_Frequency | C | 50ms | The oscillation torque frequency is below Max\_Torque\_ Frequency |
| 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 | Lane Keeping Assistance torque set to zero |

## Refined System Architecture from Functional Safety Concept

### F:\Udacity\term3\CarND-Functional-Safety-Project-master\CarND-Functional-Safety-Project-master\Architecture_Diagrams\graphic_asset_3.png

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Captures the road image stream video |
| Camera Sensor ECU - Lane Sensing | the camera system detects lane and lane departure |
| Camera Sensor ECU - Torque request generator | Request the EPS ECU to apply Torque |
| Car Display | Displays warning and information to the driver |
| Car Display ECU - Lane Assistance On/Off Status | Display if Lane Assistance function is On/Off |
| Car Display ECU - Lane Assistant Active/Inactive | Display if lane Assistance function is active or not |
| Car Display ECU - Lane Assistance malfunction warning | Display warning Lane Assistance Error |
| Driver Steering Torque Sensor | Senses the torque applied to the steering wheel |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Turns and vibrates the steering wheel according to the request received from Camera Sensor ECU |
| EPS ECU - Normal Lane Assistance Functionality | Responsible for managing Normal Lane Assistance Functionality |
| EPS ECU - Lane Departure Warning Safety Functionality | Responsible for managing Lane departure warning safety Functionality |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Responsible for managing Lane Keeping Assistance safety Functionality |
| EPS ECU - Final Torque | Responsible deriving and sending Final Torque value to the motor |
| Motor | 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 | LDW torque set to zero |
| 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 | LDW torque set to zero |
| 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 set to zero |
| 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 | LDW torque 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 | Safety Startup | LDW torque 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 torque 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 set to zero |
| 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 | LDW torque set to zero |
| 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 set to zero |
| 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 | LDW torque 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 | Safety Startup | LDW torque 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 torque is applied below ‘Max\_Duration’ | C | 500ms | LKA Safety | LKA torque set to zero |
| Technical  Safety  Requirement  02 | 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. | C | 500ms | LKA Safety | LKA torque set to zero |
| 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. | C | 500ms | LKA Safety | LKA torque set to zero |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LKA\_Torque\_Request' signal shall be ensured. | C | 500ms | Data Transmission Integrity check | LKA torque 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 | Safety Startup | LKA torque 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

For this item all the technical safety requirements allocated to the Electronic Power Steering ECU as showed in the System Architecture diagram

## 

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turning the system off (The torque request from the lane keeping assistance will be set to zero) | Malfunction\_01  Malfunction\_02 | YES | Turn on Lane Departure warning system malfunction warning light |
| WDC-02 | Turning the system off (The torque request from the lane keeping assistance will be set to zero) | Malfunction\_03 | YES | Turn on Lane Keep Assis system malfunction warning light |