

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

**[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.**

**For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 11/8/2018 | 1.0 | Sindhura Buggaveeti | Initial version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Table of Contents

**[Instructions: We have provided a table of contents. If the table of contents is not showing up correctly in your word processor of choice, please update it. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In** [**Google Docs**](https://support.google.com/docs/answer/116338?co=GENIE.Platform%3DDesktop&hl=en)**, you can use headings for each section and then go to Insert > Table of Contents.** [**Microsoft Word**](https://support.microsoft.com/en-us/help/285059/how-to-create-a-table-of-contents-by-marking-text-in-word) **has similar capabilities]**

[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

**[Instructions: Answer what is the purpose of a technical safety concept?]**

**Technical safety concept describes how the systems communicate at the message level and how the ECUs communicate with each other.**

# Inputs to the Technical Safety Concept

## Functional Safety Requirements

**[Instructions: Provide the functional safety requirements derived in the functional safety concept ]**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 requested by the LDW function is below Max\_Torque\_Amplitude | C | 50ms | LDW will set the oscillating torque amplitude to 0 |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the oscillating torque frequency requested by the LDW function is below Max\_Torque\_Frequency | C | 50ms | LDW will set the oscillating torque frequency to 0 |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied only Max\_Duration | B | 500ms | Lane keeping assistance torque is set to zero |

## Refined System Architecture from Functional Safety Concept

**[Instructions: Provide the refined system architecture from the functional safety concept]**

### 

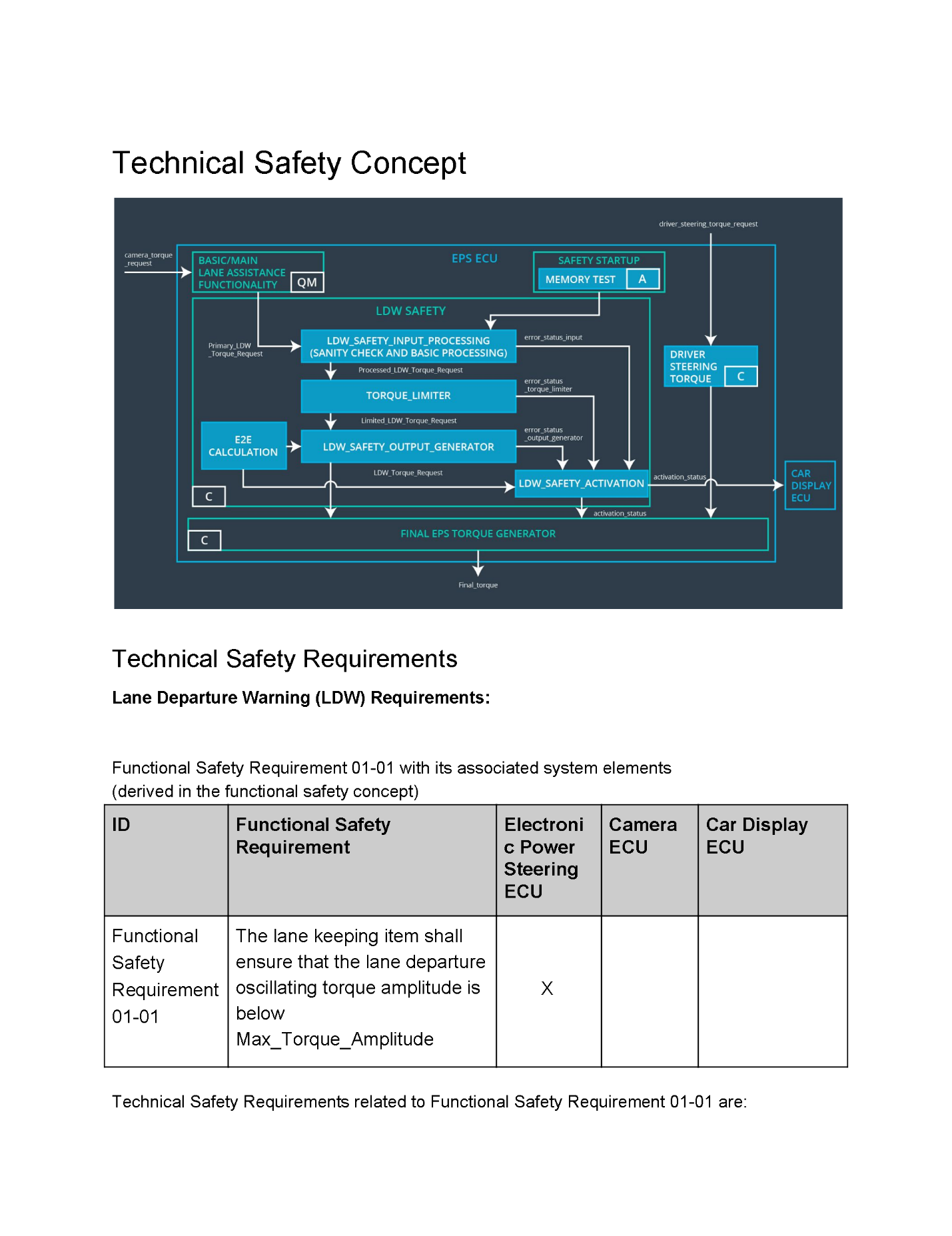
### Functional overview of architecture elements

**[Instructions: Provide a description for each functional safety element; what is each element's purpose in the lane assistance item? ]**

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Captures images and provides them to ECU |
| Camera Sensor ECU - Lane Sensing | Detects the lanes in a given camera image |
| Camera Sensor ECU - Torque request generator | Generates a torque request if the vehicle is off the current lane without turn signal from driver |
| Car Display | Displays warnings to the driver |
| Car Display ECU - Lane Assistance On/Off Status | Determine whether the lane assistance status is on/off |
| Car Display ECU - Lane Assistant Active/Inactive | Determines whether the lane assistant is active/inactive |
| Car Display ECU - Lane Assistance malfunction warning | Provides a malfunction in lane assistance functionality |
| Driver Steering Torque Sensor | Senses the torque applied by the driver to the steering wheel |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Software component that receives the torque applied by driver |
| EPS ECU - Normal Lane Assistance Functionality | Software component that receives torque request from camera sensor ECU |
| EPS ECU - Lane Departure Warning Safety Functionality | Software component that determines the oscillating torque amplitude and frequency to be applied to warn the driver of lane departure |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Software component that determines the additional torque to be applied by motors to stay in the lane |
| EPS ECU - Final Torque | Software component that determines the total torque to be applied by combining LDW and LKA torque and sends it to the motor |
| Motor | Applies the required 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 is 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 | 50ms | LDW Safety | LDW torque is 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 | 50ms | LDW safety | LDW torque is set to 0 |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for LDW\_Torque\_Request shall be set to zero | C | 50ms | Safety Startup | LDW torque is 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 the memory | A | Ignition cycle | Data transmission integrity check | LDW torque is set to 0 |

**[Instructions: Fill in the technical safety requirements for the lane departure warning second functional safety requirement. We have provided the associated functional safety requirement in the table below. Hint:. Most of the technical safety requirements will be the same. At least one technical safety requirement will have to be slightly modified because we are talking about frequency instead of amplitude. These requirements were not given in the lessons]**

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 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 is set to 0 |

**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:**

**[Instructions: Fill in the technical safety requirements for the lane keeping assistance functional safety requirement 02-01. We have provided the associated functional safety requirement in the table below. Hint:. You can reuse the technical safety requirements from functional safety requirement 01-01. But you need to change the language because we are now looking at a different system. The ASIL and Fault Tolerant Time Interval are different as well.]**

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 duration of torque applied for lane keeping assistance is below ‘Max\_Duration’ | B | 500ms | LKA Safety | LKA torque is set to 0 |
| 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 | B | 500ms | LKA Safety | LKA torque is set to 0 |
| 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 is set to 0 |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for LKA\_Torque\_Request shall be set to zero | B | 500ms | Safety Startup | LKA torque is 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 the memory | A | 500ms | Data transmission integrity check | LKA torque is set to 0 |

**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

All technical safety requirements are allocated to the Electric Power Steering ECU

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off lane departure warning functionality | Malfunction\_01  Malfunction\_02  Malfunction\_05 | Yes | Lane departure warning turn off telltale command on car Display |
| WDC-02 | Turn off lane keeping assistance | Malfunction\_03  Malfunction\_04 | Yes | Lane keeping assistance turn off tell tale command on Car Display |