

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 |
| 2017-09-19 | 1.0 | Sundeep Tuteja | Technical Safety Concept |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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?]**

The technical safety concept defines how the different subsystems interact at the message level and describes 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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude | C | 50 ms | The lane keeping item shall be disabled, output should be zero |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency | C | 50 ms | The lane keeping item shall be disabled, output should be zero |
| Functional  Safety  Requirement  02-01 | The lane keeping item shall ensure that the lane keeping assistance function torque is applied for only Max\_Duration | B | 500 ms | The lane keeping item shall be disabled, output should be 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? ]**

NOTE: The diagram above is incorrect. It shows Car Display ECU twice. The two ECUs are camera sensor ECU and car display ECU

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | The camera sensor captures images from the road |
| Camera Sensor ECU - Lane Sensing | The Lane Sensing component of the camera sensor ECU processes the image received from the camera sensor and identifies the position of the lanes that the vehicle is closest to |
| Camera Sensor ECU - Torque request generator | The Torque Request Generator component of the camera sensor ECU accepts the position of the lane from the lane sensing component relative to the vehicle, and computes an appropriate torque request for the steering wheel that would be used for both lane departure warning and lane keeping assistance. |
| Car Display | The car display displays information about the lane assistance system to the driver. |
| Car Display ECU - Lane Assistance On/Off Status | The lane assistance on/off status component in the car display ECU will determine whether or not the lane assistance system is turned on by the driver |
| Car Display ECU - Lane Assistant Active/Inactive | The lane assistant active/inactive component in the car display ECU will read messages from the camera sensor ECU to determine whether or not the lane assistance system has been activated |
| Car Display ECU - Lane Assistance malfunction warning | The lane assistance malfunction warning component in the car display ECU will read messages from the electronic power steering ECU to determine whether or not a malfunction has occurred in the lane assistance system |
| Driver Steering Torque Sensor | The driver steering torque sensor reads the torque applied to the steering wheel |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | The driver steering torque component of the electronic power steering (EPS) ECU reads the torque from the driver steering torque sensor and sends it to the final torque computation component in the EPS ECU as one of its inputs |
| EPS ECU - Normal Lane Assistance Functionality | The normal lane assistance functionality component will accept the torque from the torque request generator component of the car display ECU |
| EPS ECU - Lane Departure Warning Safety Functionality | The lane departure warning safety functionality in the EPS ECU will limit the torque amplitude and frequency to be applied |
| EPS ECU - Lane Keeping Assistant Safety Functionality | The lane keeping assistance safety functionality will limit the amount of time that the lane keeping assistance torque will be applied |
| EPS ECU - Final Torque | The final torque component in the EPS ECU will accept an input from the safety lane assistance functionality component and the driver steering torque component and process the torque value to be sent to the motor |
| Motor | The motor will apply the torque received from the EPS ECU to the steering wheel |

# Technical Safety Concept

## Technical Safety Requirements

**[Instructions: Fill in the technical safety requirements for the lane departure warning first functional safety requirement. We have provided the associated functional safety requirement in the first table below. Hint: The technical safety requirements were discussed in the lesson videos. The architecture allocation column should contain element names such as LDW Safety block, Data Transmission Integrity Check, etc. Allocating the technical safety requirements to the "EPS ECU" does not provide enough detail for a technical safety concept.]**

**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 | 50 ms | LDW safety component | LDW\_Torque\_Request should be set to 0.0 |
| 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 | 50 ms | LDW Safety | LDW\_Torque\_Request should be set to 0.0 |
| 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 | 50 ms | LDW Safety | LDW\_Torque\_Request should be set to 0.0 |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for ‘LDW\_Torque\_Request’ shall be ensured | C | 50 ms | Data Transmission Integrity Check | N/A |
| 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 (Memory Test) | LDW\_Torque\_Request should be set to 0.0 |

**[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 frequency of the LDW\_Torque\_Request sent to the ‘Final electronic power steering Torque’ component is below Max\_Torque\_Frequency | C | 50 ms | LDW safety component | LDW\_Torque\_Request should be set to 0.0 |
| 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 | 50 ms | LDW Safety | LDW\_Torque\_Request should be set to 0.0 |
| 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 | 50 ms | LDW Safety | LDW\_Torque\_Request should be set to 0.0 |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for ‘LDW\_Torque\_Request’ shall be ensured | C | 50 ms | Data Transmission Integrity Check | LDW\_Torque\_Request should be set to 0.0 |
| 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 (Memory Test) | LDW\_Torque\_Request should be set to 0.0 |

**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 the LKA\_Torque\_Request sent to the ‘Final electronic power steering Torque’ component is below Max\_Duration | B | 500 ms | LKA safety component | LKA\_Torque\_Request should be set to 0.0 |
| 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 | 500 ms | LKA Safety | LKA\_Torque\_Request should be set to 0.0 |
| 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 | 500 ms | LKA Safety | LKA\_Torque\_Request should be set to 0.0 |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for ‘LKA\_Torque\_Request’ shall be ensured | B | 500 ms | Data Transmission Integrity Check | LKA\_Torque\_Request should be set to 0.0 |
| 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 (Memory Test) | LKA\_Torque\_Request should be set to 0.0 |

**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

**[Instructions: We already included the allocation as part of the technical requirement tables. Here you can state that for this particular item, all technical safety requirements are allocated to the Electronic Power Steering ECU]**

For the lane assistance item, all technical safety requirements are allocated to the electronic power steering ECU.

## Warning and Degradation Concept

**[Instructions: 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. You can copy the functional safety warning and degradation concept here.**

**Oftentimes, a technical safety analysis will lead to a more detailed warning and degradation concept. ]**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off functionality | The lane departure warning function applies an oscillating torque with very high torque amplitude (above limit) | Yes | Warning light on the dashboard |
| WDC-02 | Turn off functionality | The lane departure warning function applies an oscillating torque with very high torque frequency (above limit) | Yes | Warning light on the dashboard |