

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 |
| 3/13/2018 | 0.5 | Tan Wang | First Draft |
| 3/19/2018 | 1.0 | Tan Wang | First Submission |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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 is a document that aims to analyze each subcomponents of subsystems and allocate risk level to each subsystem in a more detailed view, so that it can facilitate the process to avoid accidents by reducing risk to acceptable levels.**

**There could be multiple levels of technical safety concepts that addresses safety analysis in different levels of detail.**

# 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 | 50ms | The oscillating torque amplitude is set to 0 |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below max\_torque\_frequency | C | 50ms | The oscillating torque frequency is set to 0 |
| 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 | The lane keeping assistance torque is not applied |

## 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 | Gets visual perception (images and videos) of the environment |
| Camera Sensor ECU - Lane Sensing | Extracts lane lines from sensor images and calculates the real world position of lane lines |
| Camera Sensor ECU - Torque request generator | Calculates the torque required to drive the car back to the center of the lane, and send the torque request. |
| Car Display | Presents status information and warnings to drivers |
| Car Display ECU - Lane Assistance On/Off Status | Controls the display of lane assistance on/off status based on the signals from lane assistance. |
| Car Display ECU - Lane Assistant Active/Inactive | Controls the display of lane assistance active/inactive status based on the signals from lane assistance. |
| Car Display ECU - Lane Assistance malfunction warning | Controls the display of lane assistance malfunctioning status based on the signals from lane assistance. |
| Driver Steering Torque Sensor | Gets the torque applied to the steering wheel by drivers |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Converts and filters the torque value from driver steering torque sensor to the common scale/ coordinate system used in EPS ECU with a lower error/noise rate. (Like what a Kalman filter does) |
| EPS ECU - Normal Lane Assistance Functionality | Fetches the torque request from camera sensor ECU and the torque from the previous component, determine whether interventions are required. |
| EPS ECU - Lane Departure Warning Safety Functionality | Generates an oscillating torque value that vibrates the steering wheel |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Generates a torque value that turn the car to the center of the lane |
| EPS ECU - Final Torque | Combines the torque value from all previous 4 torque values and generates a final torque value to motor |
| Motor | Applies torque to the steering wheel when the car is drifting away from the lane by mistake |

# 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 components shall ensure that the amplitude of the ‘LDW\_Torque\_Request” to the “Final electronic power steering Torque’ component is below Max\_Torque\_Amplitude | C | 50ms | LDW safety components | A malfunction signal is sent |
| 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 | A malfunction signal is sent |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LDW function, it shall deactivate LDW feature and ‘LDW\_Torque\_request” shall be 0 | C | 50ms | LDW Safety components | The LDW is deactivated and the torque sent is 0 |
| Technical  Safety  Requirement  04 | As soon as the LDW function deactivates the LDW feature, the ‘LDW safety’ software block shall send a signal to car display ECU to turn on warning light | C | 50ms | LDW safety components | The warning signal is sent |
| 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 | A malfunction signal is sent |

**[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 components shall ensure that the frequency of the ‘LDW\_Torque\_Request” to the “Final electronic power steering Torque’ component is below Max\_Torque\_Frequency | C | 50ms | LDW safety components | A malfunction signal is sent |
| 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 | A malfunction signal is sent |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LDW function, it shall deactivate LDW feature and ‘LDW\_Torque\_request” shall be 0 | C | 50ms | LDW Safety components | The LDW is deactivated and the torque sent is 0 |
| Technical  Safety  Requirement  04 | As soon as the LDW function deactivates the LDW feature, the ‘LDW safety’ software block shall send a signal to car display ECU to turn on warning light | C | 50ms | LDW safety components | The warning signal is sent |
| 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 | A malfunction signal is sent |

**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 components shall ensure that the duration of LKA\_torque\_request sent to the “Final electronic power steering Torque’ is below “Max\_Duration” | B | 500ms | LKA safety components | A malfunction signal is sent |
| Technical  Safety  Requirement  02 | The validity and integrity of data transmission for ‘LKA\_Torque\_Request’ signal shall be ensured | B | 500ms | Data Transmission Integrity Check | A malfunction signal is sent |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LKA function, it shall deactivate LKA feature and ‘LKA\_Torque\_request” shall be 0 | B | 500ms | LKA Safety components | The LKA is deactivated and the torque sent is 0 |
| Technical  Safety  Requirement  04 | As soon as the LKA function deactivates the LKA feature, the ‘LKA safety’ software block shall send a signal to car display ECU to turn on warning light | B | 500ms | LKA safety components | The warning signal is sent |
| Technical  Safety  Requirement  05 | The LKA safety components shall ensure that the timer used to track the duration of applied torque is running correctly | B | 500ms | LKA safety components | A malfunction signal is sent |

**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]**

**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 the functionality | The oscillation amplitude or frequency is greater than the maximum value allowed | Yes | A warning message will be flashed on car display showing that lane departure warning system is malfunctioning |
| WDC-02 | Turn off the functionality | The LKA torque is applied for more than the maximum time allowed | Yes | A warning message will be flashed on car display showing that LKA is applied for too long, which will prompt the drivers to hold the steering wheel drive manually |