

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 |
| 9/9/2018 | 1.0 | Terry Lu | 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 concept turning functional safety requirements into technical safety requirements,

And allocating technical safety requirements to the system architecture.

# Inputs to the Technical Safety Concept

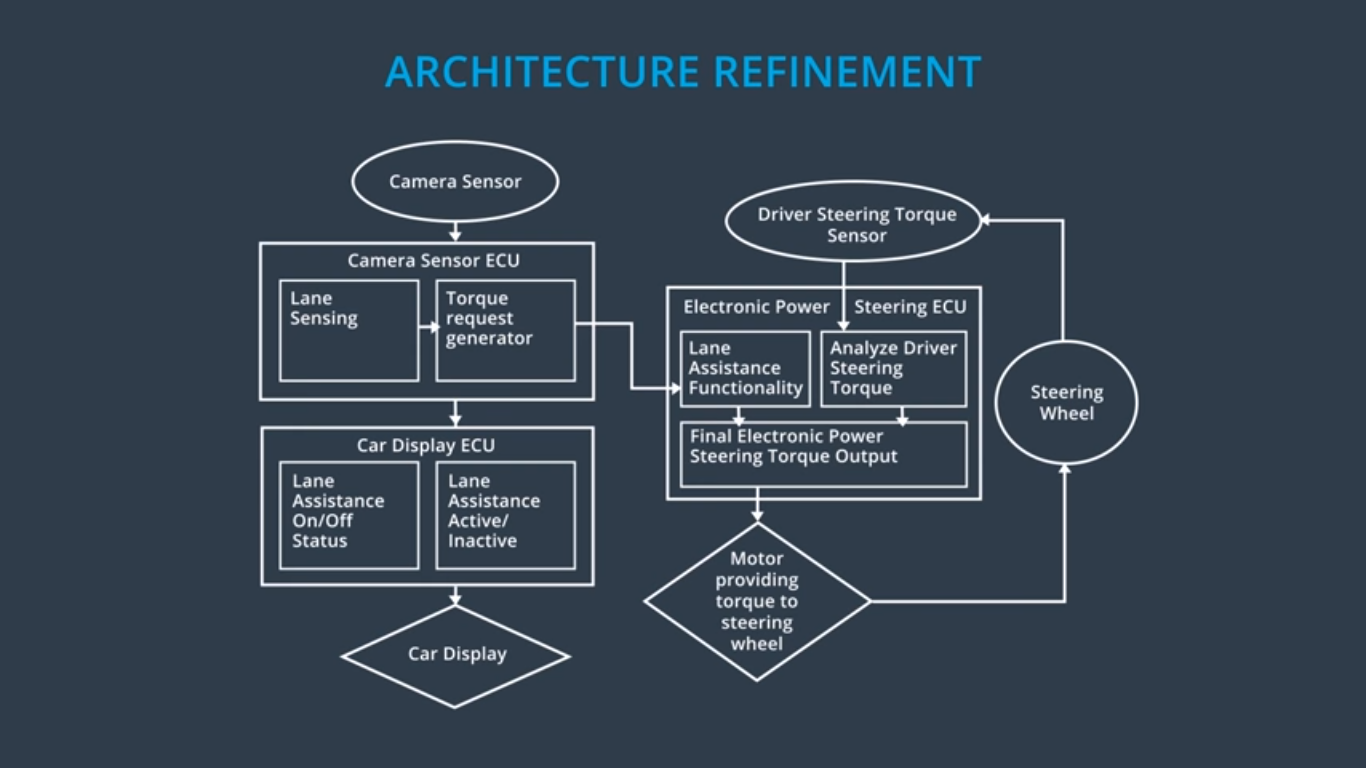
## Functional Safety Requirements

**[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 line keeping item shall ensure that the  lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude. | C | 50ms | LDW will set the  oscillating torque  amplitude to 0. |
| Functional  Safety  Requirement  01-02 | The line keeping item shall ensure that the  lane departure oscillating torque frequency is below Max\_Torque\_frequency. | C | 50ms | LDW will set the  oscillating torque  amplitude 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 | LKA will set  oscillating torque  amplitude to 0. |

## 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 | Get road image data. |
| Camera Sensor ECU - Lane Sensing | Detect the lane. |
| Camera Sensor ECU - Torque request generator | Output a reasonable torque value. |
| Car Display | Display the system status. |
| Car Display ECU - Lane Assistance On/Off Status | It controls a light that tells the driver if the lane  keeping item is on or off. |
| Car Display ECU - Lane Assistant Active/Inactive | It can tell driver if the lane departure warning is  actived. |
| Car Display ECU - Lane Assistance malfunction warning | It can receive a status signal,the signal indicates  whether or not the lane assistance itemis active  and functioning properly. |
| Driver Steering Torque Sensor | It can get acutal torque value from steering wheel. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | It can sense how much the driver is turning the  steering wheel. |
| EPS ECU - Normal Lane Assistance Functionality | It receives the vibrational request from the carema  subsystem,and it limits amplitude and frequency to  be low max torque amplitude and max torque  frequency. |
| EPS ECU - Lane Departure Warning Safety Functionality | It can apply an oscillating steering torque to provide  the driver a haptic feedback. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | It can apply the steering torque when active in  order to stay in ego lane. |
| EPS ECU - Final Torque | It adds the torque requests together to output a  final torque to the motor |
| Motor | It moves 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 Electronic Power Steering ECU shall  ensure that the oscillating torque amplitude  requested by the LDW function is below  Max\_Torque\_Amplitude. | C | 50ms | LDW Safety  block | The lane  departure  warning talk  request  amplitude  shall be 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  block | The lane  departure  warning talk  request  amplitude  shall be 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  block | The lane  departure  warning talk  request  amplitude  shall be set to  0. |
| 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. | The lane  departure  warning talk  request  amplitude  shall be set to  0. |
| Technical  Safety  Requirement  05 | Memory test shall be conducted  at startup of the EPS ECU to  check for any faults in memory. | A | ignition  cycle | Memory Test | The lane  departure  warning talk  request  amplitude  shall be 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 Electronic Power Steering ECU shall  ensure that the oscillating torque amplitude  requested by the LDW function is below  Max\_Torque\_Frequency.. | C | 50ms | LDW Safety  block | The lane  departure  warning talk  request  amplitude  shall be 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  block | The lane  departure  warning talk  request  amplitude  shall be 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  block | The lane  departure  warning talk  request  amplitude  shall be set to  0. |
| 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. | The lane  departure  warning talk  request  amplitude  shall be set to  0. |
| Technical  Safety  Requirement  05 | Memory test shall be conducted  at startup of the EPS ECU to  check for any faults in memory. | A | ignition  cycle | Memory Test | The lane  departure  warning talk  request  amplitude  shall be 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 frequency of the  lane keeping assistance torque sent to the 'Final electronic power  steering Torque' component is  below Max\_Duration. | C | 50ms | LKA Safety block | the lane assistance system  should stop  applying extra  torque after a certain amount of time. |
| 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 | 50ms | LKA Safety block | the lane assistance system  should stop  applying extra  torque after a certain amount of time. |
| Technical  Safety  Requirement  03 | As soon as a failure is detected  by the LKA function, it shall turn  off the lane keeping assistance  function. | C | 50ms | LKA Safety block | the lane assistance system  should stop  applying extra  torque after a certain amount of time. |
| Technical  Safety  Requirement  04 | The validity and integrity of the  data transmission for ' the lane  keeping assistance torque ' signal  shall be ensured. | C | 50ms | Data Transmission  Integrity Check. | the lane assistance system  should stop  applying extra  torque after a certain amount of time. |
| Technical  Safety  Requirement  05 | Memory test shall be conducted  at startup of the EPS ECU to check for any faults in memory. | A | ignition  cycle | Memory Test | the lane assistance system  should stop  applying extra  torque after a certain amount of time. |

**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. Please refer to the above table under “Technical Safety Requirements” for a detailed specification of

component architecture allocations.

## 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 | LDW disabled;  torque request  will be set to 0. | The LDW warning is giving  MORE torque  than what is  safe. | Yes | Warning light  appears on  dashboard. |
| WDC-02 | LKA disabled;  torque request  will be set to 0. | The LKA function had run above  time limit. | Yes | Warning light  appears on  dashboard. |