Elektrobit

UDACITY

# 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 |
|---|---|---|---|
| 10/10/2017 | 1.0 | Sung jin , kwon | First draft |
| | | | |
| | | | |
| | | | |
| | | | |

# 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, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]**

# Purpose of the Technical Safety Concept

**[Instructions: Answer what is the purpose of a technical safety concept?]**
The Technical Safety Concept defines how the subsystems interact at the signal level and describes how the ECUs communicate each other.

So the technical safety concept involves:
Turning functional safety requirements into technical safety requirements.
Allocating each technical safety requirements to the system architecture.

# Inputs to the Technical Safety Concept

## Functional Safety Requirements

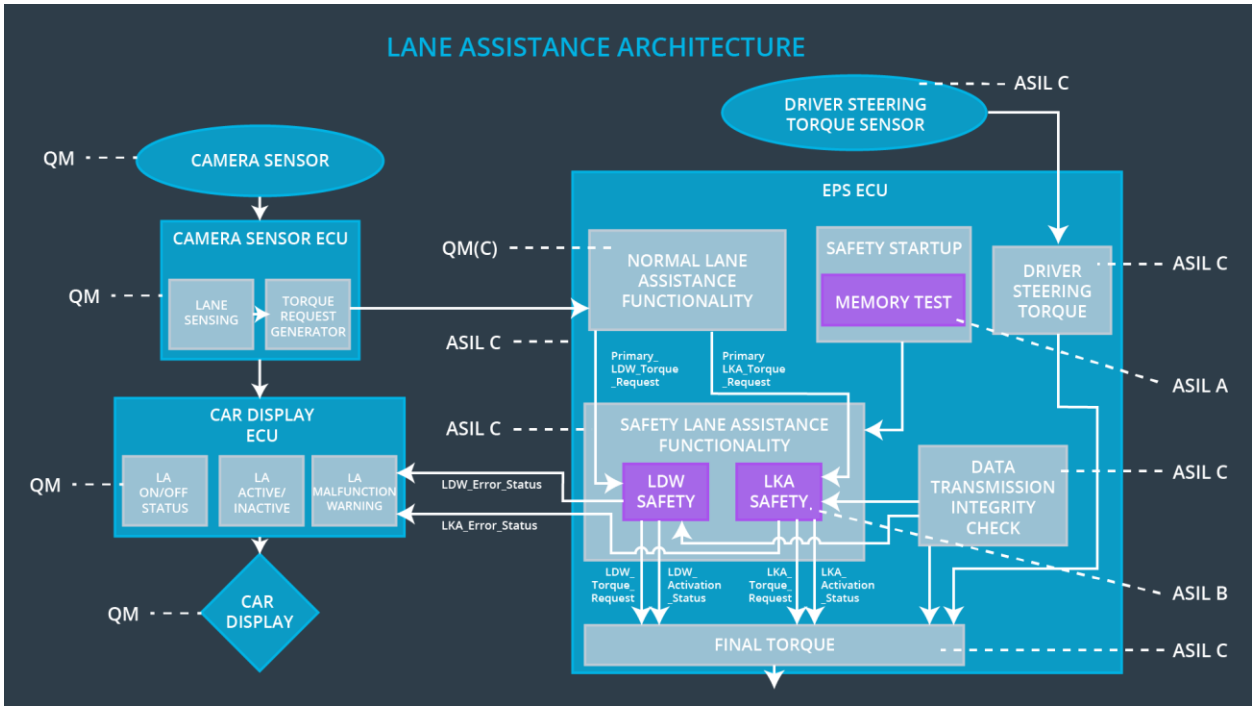
**[Instructions: Provide the functional safety requirements derived in the functional safety concept ]**

| ID | Functional Safety Requirement | ASIL | Fault Tolerant Time Interval | Safe State |
|---|---|---|---|---|
| Functional Safety Requirement 01-01 | The electronic power steering ECU shall ensure that the lane departure warning 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 electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency is below Max_Torque_Frequency | C | 50ms | LDW will set the oscillating torque frequency to 0 |
| Functional Safety Requirement | The electronic power steering ECU shall ensure that the lane keeping assistance | C | 50ms | LKA system is deactivated |

| | | | | |
|---|---|---|---|---|
| 02-01 | torque is applied for only Max_Duration | | | |

# 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 images |
| Camera Sensor ECU - Lane Sensing | Detect lane line from image and measure the distance between car center and lane center |

| | |
|---|---|
| Camera Sensor ECU - Torque request generator | Sends a torque request to the power steering ECU |
| Car Display | Device that displays symbol or picture |
| Car Display ECU - Lane Assistance On/Off Status | Receives a signal from the power steering ECU about the status of the lane departure warning function and send display information to Car Display |
| Car Display ECU - Lane Assistant Active/Inactive | Receives a signal from the power steering ECU about the status of the lane Assistant Active/Inactive and send display information to Car Display |
| Car Display ECU - Lane Assistance malfunction warning | Receives a signal from the power steering ECU if there is a malfunction with the lane assistance system and send display information to Car Display |
| Driver Steering Torque Sensor | Senses how much torque is already being applied by the driver |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Determines how much torque is already being applied by the driver |
| EPS ECU - Normal Lane Assistance Functionality | Receives LDW or LKA torque request from the camera ECU and compute appropriate torque signal |
| EPS ECU - Lane Departure Warning Safety Functionality | Check if the computed torque of Normal Lane Assistance Functionality is within limited range. If not, generate error signal and set torque to 0. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Check if the torque request duration of Normal Lane Assistance Functionality is within limited range. If not, generate error signal and set torque to 0. |
| EPS ECU - Final Torque | Output torque signal from Lane Departure Warning Safety Functionality or Lane Keeping Assistant Safety Functionality |
| Motor | Applies physical torque 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 | 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 Block | Final Torque shall be set to zero |

| | | | | | |
|---|---|---|---|---|---|
| Technical Safety Requirement 02 | Validity and Integrity of the data transmission for the LDW_Torque_Request signal shall be ensured | C | 50ms | Data Transmission Integrity Check | Final Torque shall be 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 Block | Final Torque shall be set to zero |
| Technical Safety Requirement 04 | 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 | Final Torque shall be set to zero |
| Technical Safety Requirement 05 | Memory test shall be conducted at the startup of EPS ECU | A | Ignition cycle | Separate External block with Memory | Final Torque shall be set to zero |

**[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 | 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 | 50ms | LDW Safety Component | Final Torque shall be set to zero |
| Technical Safety Requirement 02 | Validity and Integrity of the data transmission for the LDW_Torque_Request signal shall be ensured | C | 50ms | Data Transmission Integrity Check | Final Torque shall be 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 Component | Final Torque shall be set to zero |
| Technical Safety Requirement 04 | 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 | Final Torque shall be set to zero |
| Technical Safety Requirement 05 | Memory test shall be conducted at the startup of EPS ECU to check for any faults in memory. | A | Ignition Cycle | Separate External block with Memory test code | Final Torque shall be set to zero |

**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 | | |

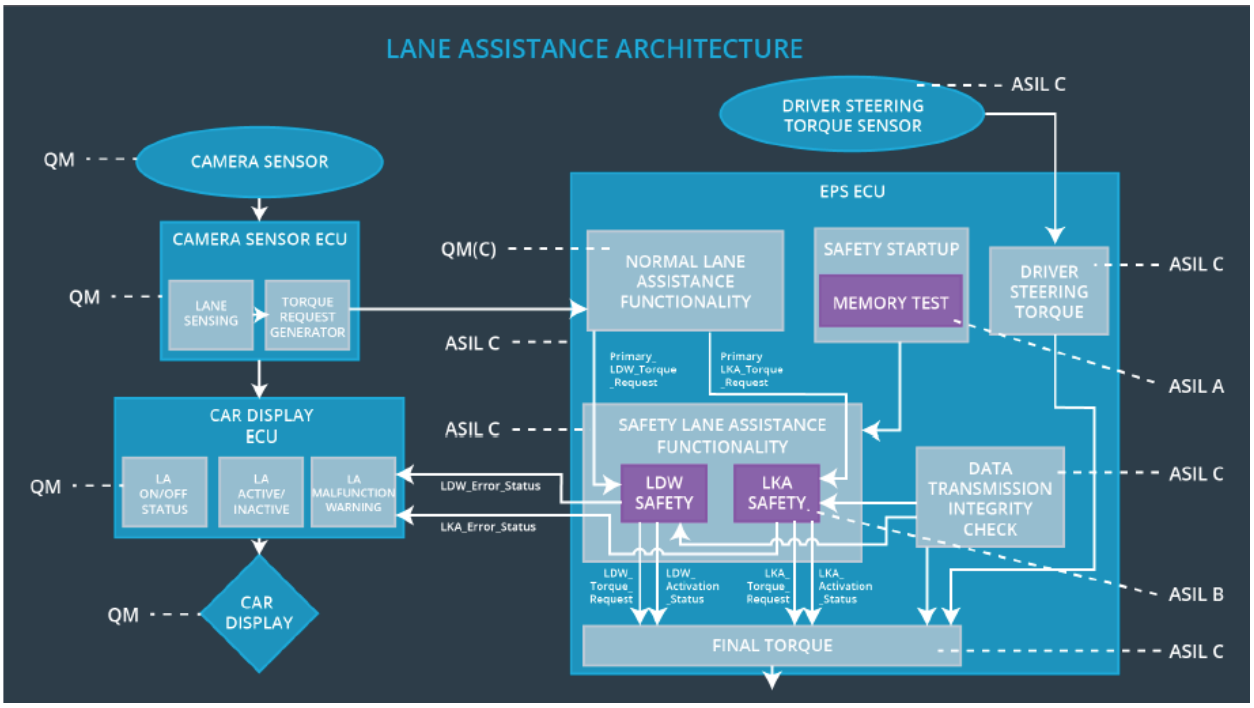
Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

| ID | Technical Safety Requirement | ASIL | Fault Tolerant Time Interval | Allocation to Architecture | Safe State |
|---|---|---|---|---|---|
| Technical Safety Requirement 01 | 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_torque_duration | B | 500ms | LKA safety component | Final Torque shall be set to zero |
| Technical Safety Requirement 02 | Validity and Integrity of the data transmission for the LKA_Torque_Request signal shall be ensured | B | 500ms | Data Transmission Integrity Check | Final Torque shall be 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 | B | 500ms | LKA safety component | Final Torque shall be set to zero |

| | | | | | |
|---|---|---|---|---|---|
| | be set to zero. | | | | |
| Technical Safety Requirement 04 | 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 component | Final Torque shall be set to zero |
| Technical Safety Requirement 05 | Memory test shall be conducted at the startup of EPS ECU to check for any faults in memory. | A | Ignition Cycle | Separate External block with Memory test code | Final Torque shall be set to zero |

## 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]**

## 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. ]**

| | |
|---|---|
| Warning | Warning light displayed to the driver on the dashboard |
| Degradation | Turn off functionality |