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 |
|---|---|---|---|
| 25 June 2019 | 1.0 | Guilin Zhu | First 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, 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 purpose of technical safety concept is to turn functional safety requirements into technical safety requirements and allocate technical safety requirements to the system architecture

# Inputs to the Technical Safety Concept

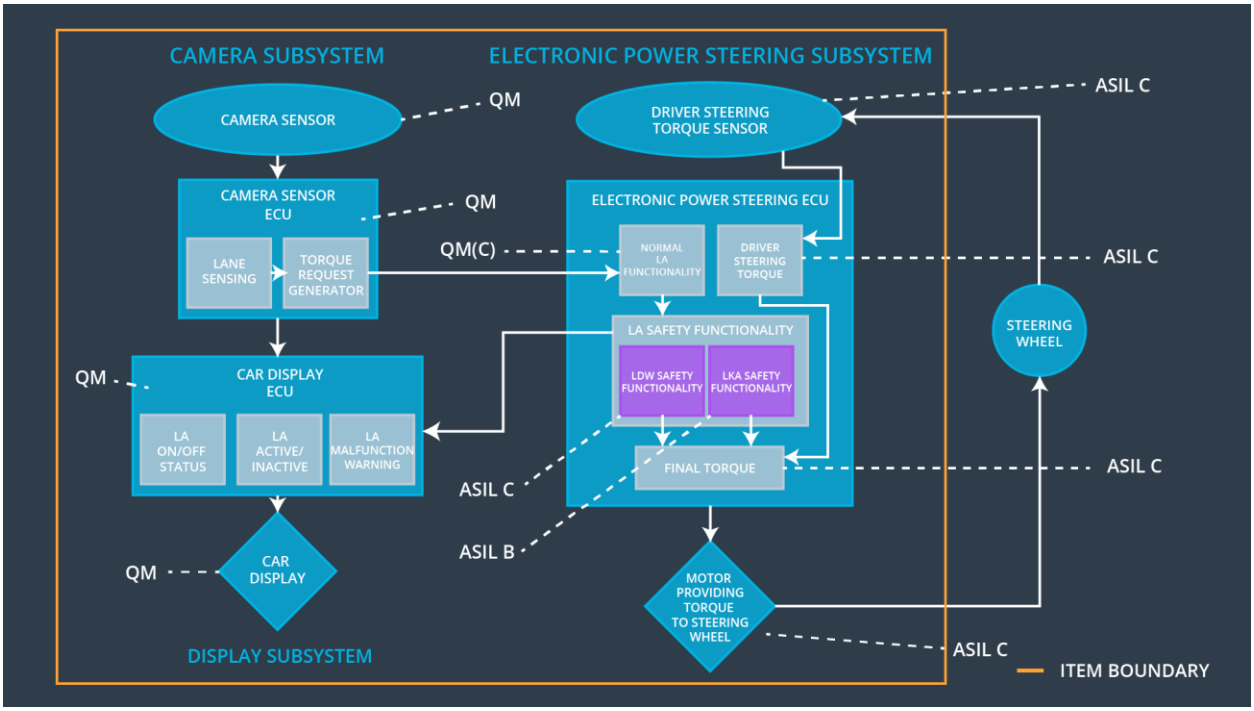
## Functional Safety Requirements

**[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 electric power steering ECU shall ensure the lane departure oscillating torque amplitude is below Max_Torque_Amplitude | C | 50ms | LDW off |
| Functional Safety Requirement 01-02 | The electric power steering ECU shall ensure that lane departure oscillating torque frequency is below Max_Torque_Frequency | C | 50ms | LDW off |
| Functional Safety Requirement 02-01 | The electric power steering subsystem shall ensure that LKA function is able to detect driver hands off the wheel for Max_duration | B | 500ms | LKA off |
| Functional Safety Requirement 02-02 | The EPS shall ensure that LKA function torque output is below Max_Cmd | B | 500ms | Warn the driver and LKA off |

## 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 | Responsible for getting the images of external objects |
| Camera Sensor ECU - Lane Sensing | Sense where the lane mark is |
| Camera Sensor ECU - Torque request generator | Provide the oscillating torque to the EPS |
| Car Display | Display the warning of LKA/LDW status |
| Car Display ECU - Lane Assistance On/Off Status | Display the state of lane assistance active/inactive |
| Car Display ECU - Lane Assistant Active/Inactive | Display warning of lane assistant active/inactive |

| | |
|---|---|
| Car Display ECU - Lane Assistance malfunction warning | Display warning for malfunction of lane assistance |
| Driver Steering Torque Sensor | Detect the driver handwheel torque and provide the haptic feedback |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Provide the steering torque command to the motor |
| EPS ECU - Normal Lane Assistance Functionality | Process the normal lane assistance function and output the torque command |
| EPS ECU - Lane Departure Warning Safety Functionality | Safety check on the LDW torque command and provide the status of LDW |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Safety check on the LKA torque command and provide the status of LKA |
| EPS ECU - Final Torque | The output of torque command after safety checks |
| Motor | Excute the torque command from EPS ECU and Provide the motion |

# 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 | The EPS shall ensure that the lane departure oscillating torque | X | | |

| | | | | |
|---|---|---|---|---|
| Requirement 01-01 | amplitude is below Max_Torque_Amplitude | | | |

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 component | LDW off |
| 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 | Warn the driver and LDW off |
| 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 | Warn the driver of malfunction and LDW off |
| 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 | LDW off |
| 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 | EPS ECU | LDW off |

**[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 EPS 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_Frequency. | C | 50ms | LDW safety component | LDW off |
| Technical Safety Requirement 02 | As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block shall | C | 50ms | LDW safety | LDW off |

| | | | | | |
|---|---|---|---|---|---|
| | send a signal to the car display ECU to turn on a warning light. | | | | |
| 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 off |
| 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 | LDW off |
| 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 | EPS ECU | LDW off |

**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 electric power steering subsystem shall ensure that LKA function is able to detect driver hands off the wheel for Max_duration | X | | 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 EPS shall report hands-off state (steering wheel hands off detection state=$0, hands-off) not later than Max_duration seconds after the driver has taken off the hands from the steering wheel | B | 500ms | Steering torque sensor; EPS ECU | Warn the driver |
| Technical Safety Requirement 02 | The EPS shall report HOD fault if it’s incapable to detect hands-off or on. | B | 500ms | EPS ECU | Warn the driver of malfunction and LKA off |
| Technical Safety Requirement 03 | 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 | EPS<br>LKA safety block | LKA off |
| Technical Safety Requirement 04 | The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured. | B | 500ms | Data transmission integrity check | LKA off |

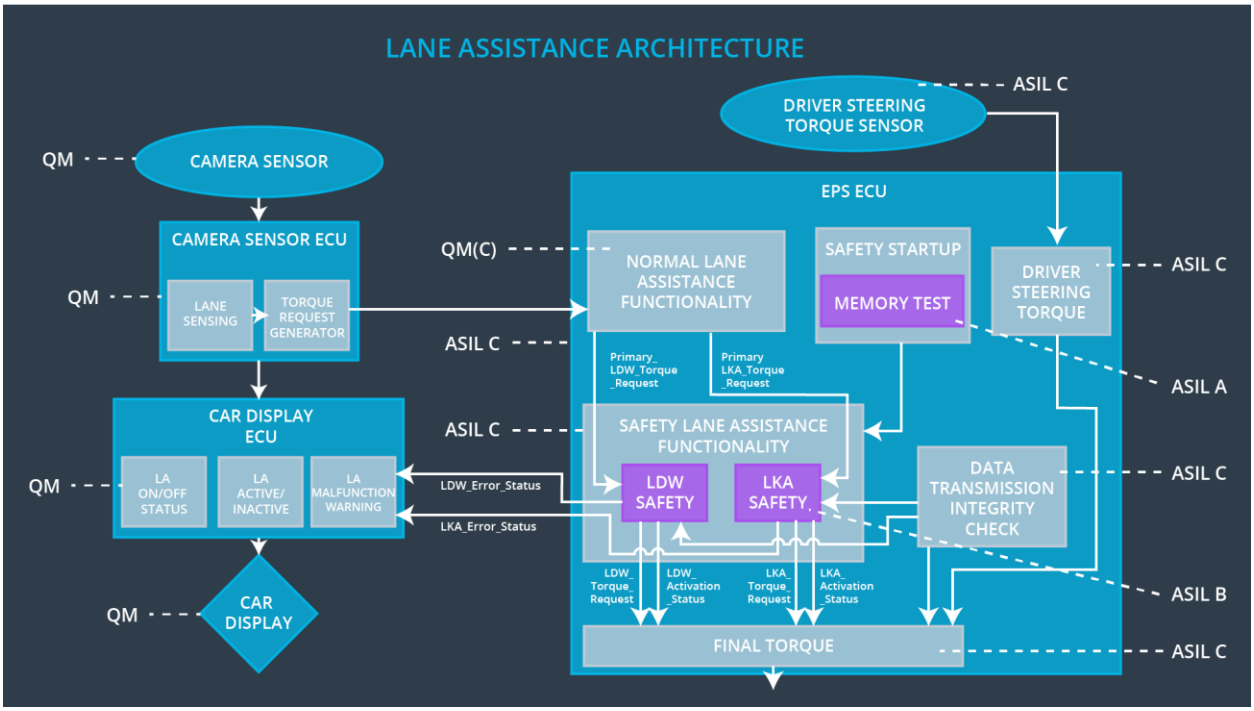
| | | | | | |
|---|---|---|---|---|---|
| Technical Safety Requirement 05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | A | Ignition cycle | EPS ECU | LKA off |

**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 above have been allocated to the system architecture elements.

## 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. ]**