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 |
|---|---|---|---|
| 2017-12-26 | 1.0 | Sven Eriksson | Initial release |
| 2017-12-26 | 2.0 | Sven Eriksson | Changes to LKA requirement ASIL level and the Warning and Degradation concept (after feedback from Udacity) |
| | | | |
| | | | |
| | | | |

# 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 the technical safety concept is to further analyze the item to identify new requirements and allocate these to system diagrams. The technical safety concept focuses more on the implementation than the functional safety concept. The technical safety concept analysis accounts for more details about the sensors, control units and actuators. The outcome of the technical safety concept are general hardware and software technical safety requirements.

# Inputs to the Technical Safety Concept

## Functional Safety Requirements

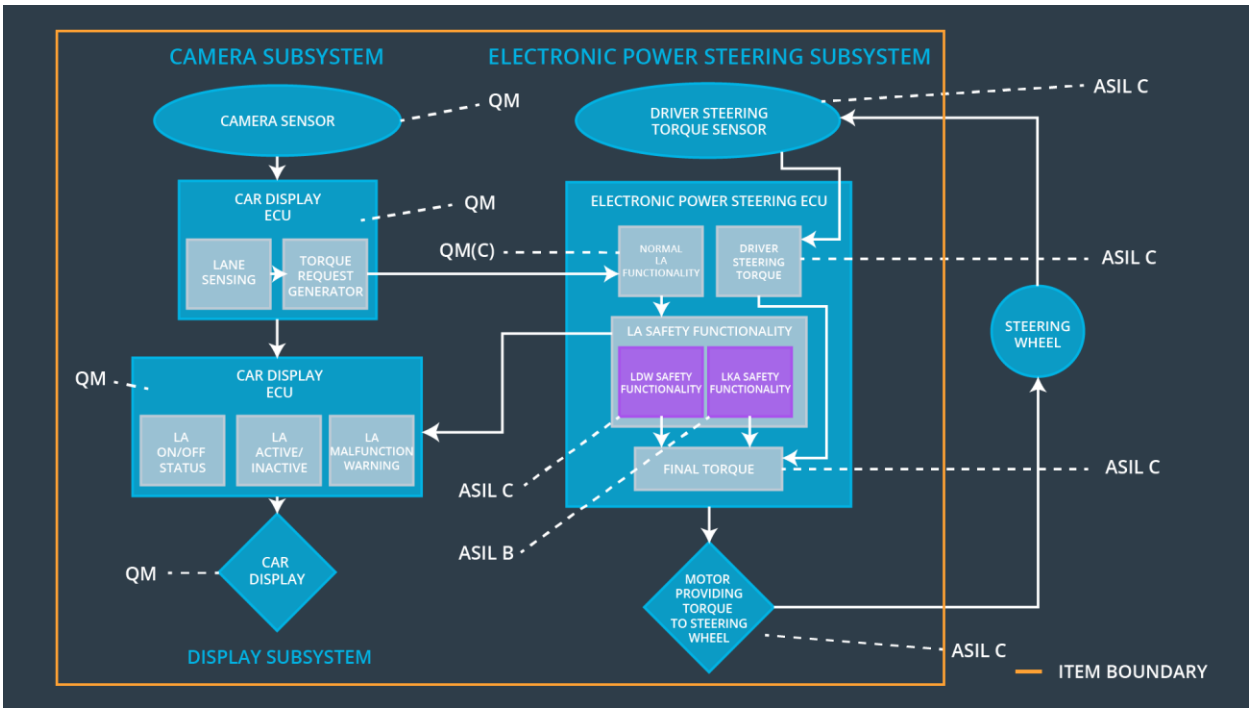
**[Instructions: Provide the functional safety requirements derived in the functional safety concept ]**

| 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 oscillating torque amplitude is below Max_Torque_Amplitude | C | 50 mS | System turned off, no torque is being applied by the system. |
| Functional Safety Requirement 01-02 | The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below | C | 50 mS | System turned off, no torque is being applied by the system. |

| | | | | |
|---|---|---|---|---|
| | Max_Torque_Frequency | | | |
| 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 | 500 mS | System turned off, no torque is being applied by the system. |

## 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 | To capture an image of the road in front of the vehicle. |
| Camera Sensor ECU - Lane Sensing | To process the image and calculate the vehicle's position and orientation within the lane. |
| Camera Sensor ECU - Torque request generator | To generate a torque request based on the vehicle's position and orientation within the lane. |
| Car Display | To display information to the driver regarding the state of the lane assistance item. |
| Car Display ECU - Lane Assistance On/Off Status | To display if the lane assistance function is on or off. |
| Car Display ECU - Lane Assistant Active/Inactive | To display if the lane assistance function is currently active or inactive. |
| Car Display ECU - Lane Assistance malfunction warning | To display any warnings from the lane assistance item. |
| Driver Steering Torque Sensor | To display if the lane assistance function is on or off. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | To measure the torque that the driver applies on the steering wheel. |
| EPS ECU - Normal Lane Assistance Functionality | To receive the torque request from the "Camera Sensor ECU - Torque request generator" and forward it to "LA safety functionality". |
| EPS ECU - Lane Departure Warning Safety Functionality | To limit the amplitude and frequency of the torque request. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | To limit the time that torque is applied. |
| EPS ECU - Final Torque | To account for driver torque and outputting the correct torque request to the motor. |
| Motor | To apply the requested 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 | 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 | ‘LDW_Torque_Request’ amplitude shall be set to zero. |
| Technical Safety Requirement 02 | The validity and integrity of the data transmission for ‘LDW_Torque_Request’ signal shall be ensured. | C | 50ms | Data transmission integerity check | ‘LDW_Torque_Request’ amplitude shall be set to zero. |

| | | | | | |
|---|---|---|---|---|---|
| Technical Safety Requirement 03 | As soon as a failure is detected by the LDW function, it shall deactive the LDW feature and the 'LDW_Torque_Request' shall be set to zero. | C | 50ms | LDW Safety | 'LDW_Torque_Request' amplitude 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 | 'LDW_Torque_Request' amplitude shall be set to zero. |
| Technical Safety Requirement 05 | Memory test shall be conducted at start up of the EPC ECU to check for any faults in memory. | A | ignition cycle | Memory test | 'LDW_Torque_Request' amplitude 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 | 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 | 'LDW_Torque_Request' amplitude shall be set to zero. |
| Technical Safety Requirement 02 | The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured. | C | 50ms | Data transmission integerity check | 'LDW_Torque_Request' amplitude shall be set to zero. |
| Technical Safety Requirement 03 | As soon as a failure is detected by the LDW function, it shall deactive the LDW feature and the 'LDW_Torque_Request' shall be set to zero. | C | 50ms | LDW Safety | 'LDW_Torque_Request' amplitude 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 | 'LDW_Torque_Request' amplitude shall be set to zero. |
| Technical Safety Requirement 05 | Memory test shall be conducted at start up of the EPC ECU to check for any faults in memory. | A | ignition cycle | Memory test | 'LDW_Torque_Request' amplitude shall be set to zero. |

**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 Requireme | The LKA safety component shall ensure that the lane keeping assistance torque is applied for | B | 500ms | LKA Safety | 'LKA_Torque_Request' amplitude |

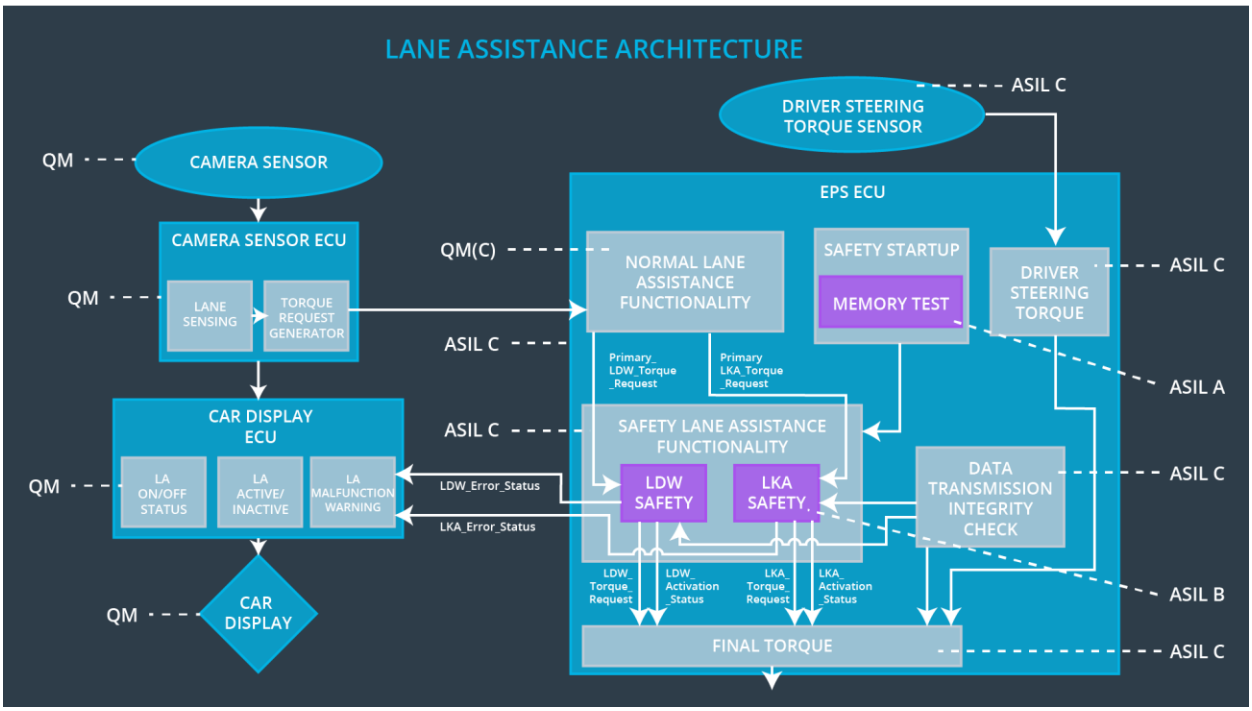
| | | | | | |
|---|---|---|---|---|---|
| nt 01 | only Max_Duration | | | | shall be set to zero. |
| Technical Safety Requirement 02 | The validity and integrity of the data transmission for ‘LKA_Torque_Request’ signal shall be ensured. | B | 500ms | Data transmission integerity check | ‘LKA_Torque_Request’ amplitude shall be set to zero. |
| Technical Safety Requirement 03 | As soon as a failure is detected by the LDW function, it shall deactive the LDW feature and the ‘LDW_Torque_Request’ shall be set to zero. | B | 500ms | LKA Safety | ‘LKA_Torque_Request’ amplitude 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. | B | 500ms | LKA Safety | ‘LKA_Torque_Request’ amplitude shall be set to zero. |
| Technical Safety Requirement 05 | Memory test shall be conducted at start up of the EPC ECU to check for any faults in memory. | A | ignition cycle | Memory test | ‘LKA_Torque_Request’ amplitude shall be set to zero. |

**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 assistant item all technical safety requirements are allocated to various parts of 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 | LDW_Activation_Status = inactive LDW_Torque_Request = 0 | LDW_Torque_Request amplitude higher than Max_Torque_Amplitude | Yes | Warning light disabled on car display |
| WDC-02 | LDW_Activation_Status = inactive LDW_Torque_Request = 0 | LDW_Torque_Request frequency higher than Max_Torque_Frequency | Yes | Warning light disabled on car display |
| WDC-03 | LKA_Activation_status = inactive LKA_Torque_Request = 0 | LKA_Activation_Status has been active for more than Max_Duration | Yes | Warning light on the car display |