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 |
|---|---|---|---|
| 20-Dec-2017 | 1.0 | Carsten MIELENZ | 1st 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?]**
**lesson 18 – 1**

The Technical Safety Plan defines how the subsystems of the item interact at the message level and specifies how the ECUs communicate to each other.
It tunes the safety requirements from the Function Safety Concept - tuning requirements from concept to development level - and allocates these technical requirements to the system architecture.

# Inputs to the Technical Safety Concept

## Functional Safety Requirements

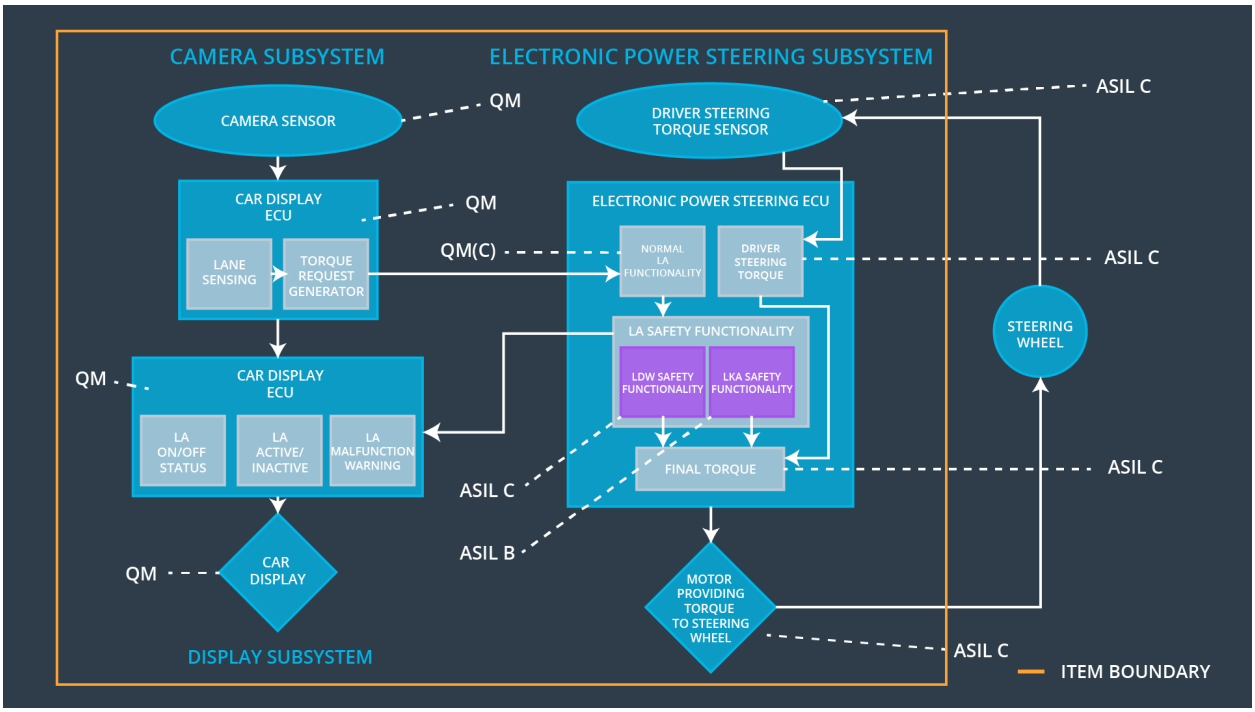
**[Instructions: Provide the functional safety requirements derived in the functional safety concept ]**
**4**

| 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 | 50ms | zero torque |
| Functional Safety Requirement 01-02 | The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency | C | 50ms | zero torque |

| | | | | |
|---|---|---|---|---|
| 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 | zero torque |

## 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 | The Camera Sensor takes a picture of the lane and send it to the Camera Senor ECU. |

| | |
|---|---|
| Camera Sensor ECU - Lane Sensing | The Camera Sensor ECU senses the picture from the Camera Sensor for lane departure. In case of lane departure is send an departure info “LA Active” to the Car Display ECU and triggers the Torque request generator. |
| Camera Sensor ECU - Torque request generator | The torque request generator generate the vibrational torque request sent EPS ECU |
| Car Display | The Car Display receives message display request form the Car Display ECU. The messages are “LA Active/Inactive”, “LA Malfunction Warning”, “LA On/Off Status” |
| Car Display ECU - Lane Assistance On/Off Status | The Car Display ECU receives “LA Off Status” message form the EPS ECU. It send a message display request to the Car Display. else it sends a “LA On Status” to the Car Display. |
| Car Display ECU - Lane Assistant Active/Inactive | The Car Display receives Lane Departure message from the Camera Sensor ECU and sends “LA Active” to the Car Display, else it sends a “LA Inactive message” to the Car Display. |
| Car Display ECU - Lane Assistance malfunction warning | The Car Display ECU receives “LA Malfunction Warning” message form the EPS ECU. It send a message display request to the Car Display. |
| Driver Steering Torque Sensor | The Car Driver Steering Torque Sensor senses how much the steering wheel is turned and sends the result to the EPS ECU. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | It analyzes the driver sensor result from the Car Driver Steering Torque Sensor and send a corresponding steering torque request to the Final Torque. |
| EPS ECU - Normal Lane Assistance Functionality | It receives a torque request from the Camera Sensor ECU and triggers Lane Departure Warning Safety Functionality and the Lane Keeping Assistant Safety Functionality to execute. |
| EPS ECU - Lane Departure Warning Safety Functionality | It receives a torque vibrate request from the Normal Lane Assistance Functionality and checks if the amplitude and frequency of the torque request is in the limits. If yes it sends this torque request to Final Torque. If not it sends zero torque to Final Torque and sends a “LA Malfunction Warning” message to the Car Display ECU. |
| EPS ECU - Lane Keeping Assistant | It receives a lane keeping torque request from the |

| | |
|---|---|
| Safety Functionality | Normal Lane Assistance Functionality. It checks if that torque is applied within time interval of Max_Duration. If the time crosses the Max_Duration time interval it sends a zero torque to Final Torque and sends a “LA Off Status” message to the Car Display ECU. If time is smaller or equal to Max_Duration time interval it sends the torque to Final Torque and sends a “LA On Status” message to the Car Display ECU. |
| EPS ECU - Final Torque | It receives torques requests from the Lane Departure Warning Safety Functionality, Lane Keeping Assistant Safety Functionality and Driver Steering Torque and calculates a final steering wheel torque request which is sent to the Motor |
| Motor | Based on the torque request of the EPS ECU the Motor provides the final 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 Functionality | The LDW torque request amplitude shall be set to zero |
| 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 Functionality | The 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 deactivate the LDW feature and the 'LDW_Torque_Request' shall be set to zero. | C | 50ms | LDW Safety Functionality | The LDW torque request amplitude shall be set to zero |
| 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 | N/A |
| 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 of vehicle | Safety Startup Test | The 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 amplitude of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency. | C | 50ms | LDW Safety Functionality | The LDW torque request amplitude shall be set to zero |
| 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 Functionality | The 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 deactivate the LDW feature and the 'LDW_Torque_Request' shall be set to zero. | C | 50ms | LDW Safety Functionality | The LDW torque request amplitude shall be set to zero |
| 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 | N/A |
| 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 of vehicle | Safety Startup Test | The 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 Requirement 01 | The LKA safety component shall ensure lane keeping assistance torque of 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is applied for *Max_Duration* time interval only. | B | 500ms | LKA Safety Functionality | The LKA torque request amplitude shall be set to zero |
| 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 LA Off Status. | B | 500ms | LKA Safety Functionality | The LKA torque request amplitude 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 be set to zero. | B | 500ms | LKA Safety Functionality | The LKA torque request amplitude shall be set to zero |

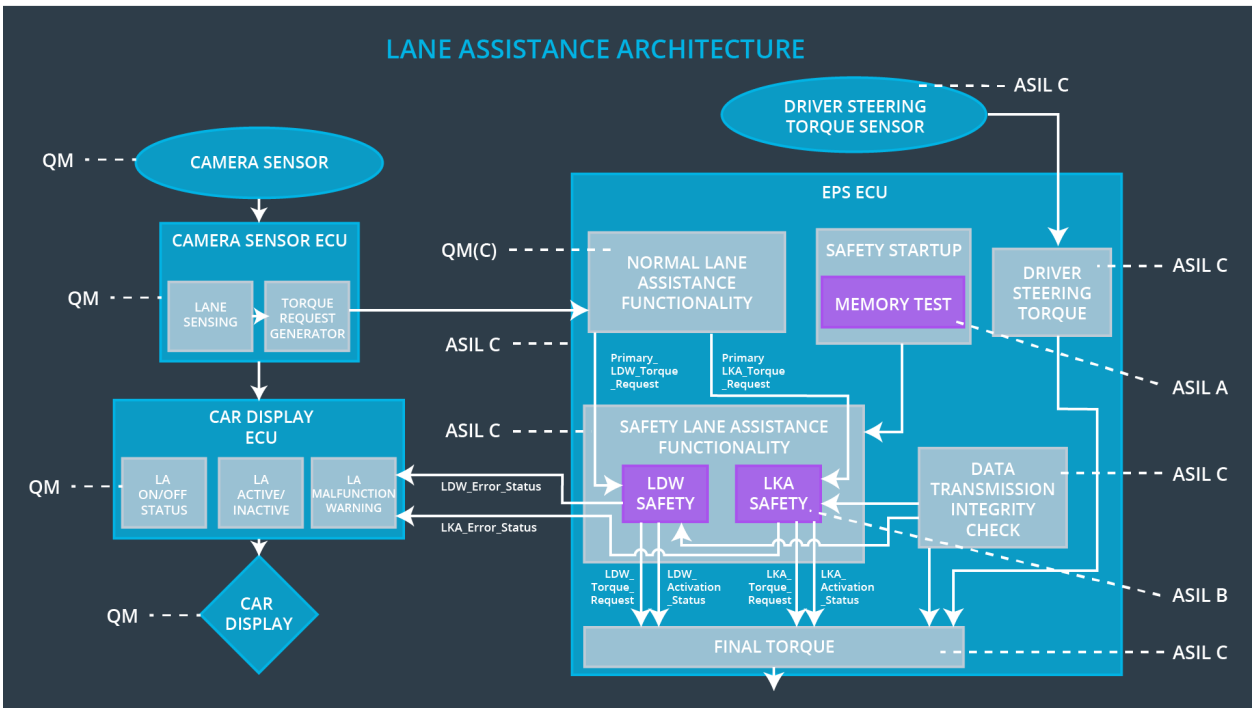
| | | | | | |
|---|---|---|---|---|---|
| Technical Safety Requirement 04 | The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured. | B | 50ms | Data Transmission Integrity Check | N/A |
| ~~Technical Safety Requirement 05~~ | ~~Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.~~<br><br>REMARK: Only needed for ASIL C or D. | ~~A~~ | ~~Ignition cycle of vehicle~~ | ~~Safety Startup Test~~ | ~~The 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]**

## 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 function | Malfunction_01 or Malfunction_02 | Yes | Lane Assist Malfunction |
| WDC-02 | Turn-off function | Malfunction_03 | Yes | Lane Assist not designed for autonomous driving |