Elektrobit

UDACITY

# Software Safety Requirements and Architecture

## 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 |
|---|---|---|---|
| 11/04/2018 | 1.0 | BM | First version of the document |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents

# Purpose

The purpose of this document is to provide the software safety requirements based on the technical safety requirements written in the technical safety concept document. The software safety requirements provided in this document can serve the software engineers as concrete and precise instructions during the product development.

# Inputs to the Software Requirements and Architecture Document

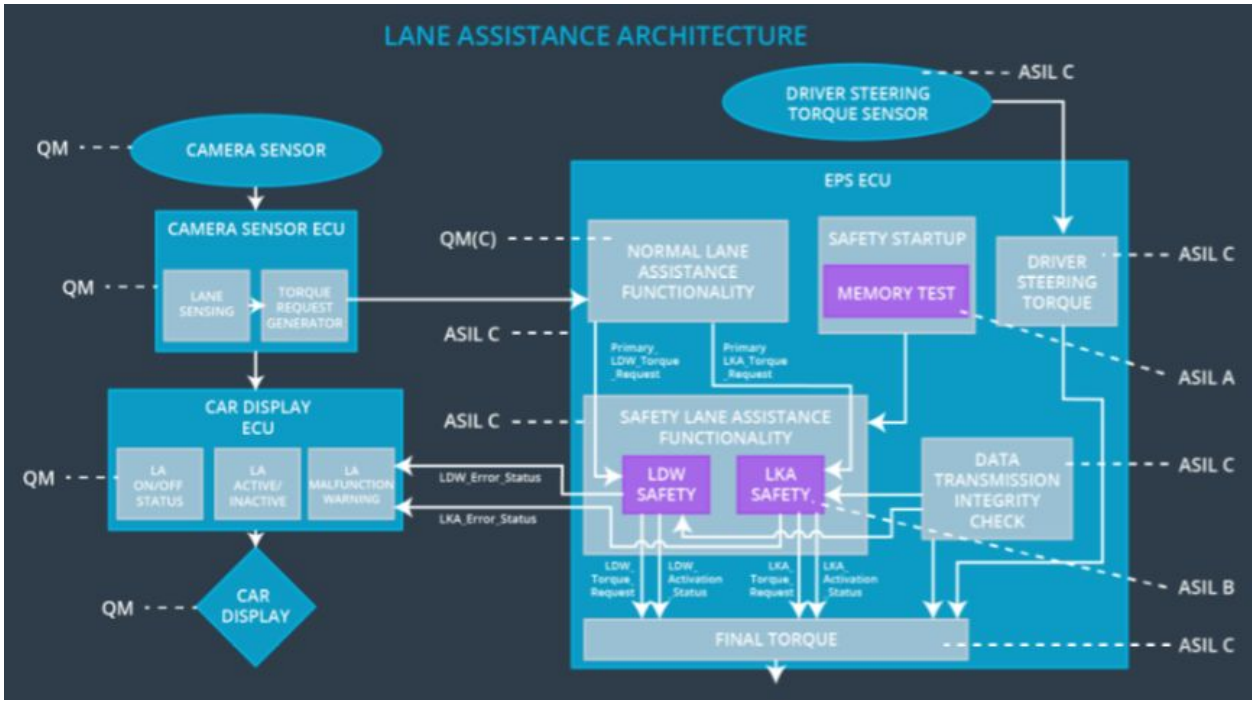
## Technical safety requirements

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 maximum amplitude of the “LDW_Torque_Request” value, which is sent to the “Final electronic power steering Torque” component, is below the maximum allowed value “Max_Torque_Amplitude” | C | 50 ms | LDW safety | LDW_Torque_Request is set to zero |
| Technical Safety Requirement 02 | When the LDW function is deactivated, the LDW safety component shall send a signal to the car display ECU to turn on a warning signal. | C | 50 ms | LDW safety | LDW_Torque_Request is set to zero |

| | | | | | |
|---|---|---|---|---|---|
| Technical Safety Requirement 03 | When the LDW safety component detects a failure, it shall deactivate the LDW function and permanently set “LDW_Torque_Request” to zero. | C | 50 ms | LDW safety | LDW_Torque_Request is set to zero |
| Technical Safety Requirement 04 | The validity and integrity of the data transmission for “LDW_Torque_Request” signal shall be ensured. | C | 50 ms | Data transmission integrity check | LDW_Torque_Request is set to zero |
| Technical Safety Requirement 05 | Memory test shall be conducted at start up of the electronic power steering ECU, to check for any memory problems | A | Ignition cycle | Memory check | LDW_Torque_Request is set to zero |

## Refined Architecture Diagram from the Technical Safety Concept




# Software Requirements

**Lane Departure Warning (LDW) Amplitude Malfunction Software Requirements:**

| ID | Technical Safety Requirement | ASIL | Fault Tolerant Time Interval | Allocation to Architecture | 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 | 50 ms | LDW safety | LDW_Torque_Request is set to zero |

| ID | Software Safety Requirement | ASIL | Allocation Software Elements | Safe State |
|---|---|---|---|---|
| Software Safety Requirement 01-01 | The input signal ‘Primary_LDW_Torq_Req’ shall be read and pre-processed to determine the torque request coming from the ‘Basic/Main LAFunctionality’ SW Component. Signal ‘processed_LDW_Torq_Req’ shall be generated at the end of the processing. | C | LDW_SAFETY_INPUT_PROCESSING | N/A |
| Software Safety Requirement 01-02 | In case the ‘processed_LDW_Torq_Req’ signal has a value greater than ‘Max_Torque_Amplitude_LDW’ (maximum allowed safe torque), the torque signal ‘limited_LDW_Torq_Req’ shall be set to zero, else ‘limited_LDW_Torq_Req’ shall take the value of ‘processed_LDW_Torq_Req’ | C | TORQUE_LIMITER | ‘limited_LDW_Torq_Req’ = 0 |
| Software Safety Requirement 01-03 | The ‘limited_LDW_Torq_Req’ shall be transformed into a signal ‘LDW_Torq_Req’ which is suitable to be transmitted outside the LDW Safety component (‘LDW Safety’) to the ‘Final EPS Torque’ component. | C | LDW_SAFETY_OUTPUT_GENERATOR | LDW_Torq_Req = 0 |

| ID | Technical Safety Requirement | ASIL | Fault Tolerant Time Interval | Allocation to Architecture | Safe State |
|---|---|---|---|---|---|
| Technical Safety Requirement 02 | The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured | C | 50 ms | Data transmission integrity check | LDW_Torque_Request is set to zero |

| ID | Software Safety Requirement | ASIL | Allocation Software Elements | Safe State |
|---|---|---|---|---|
| Software Safety Requirement 02-01 | Any data to be transmitted outside of LDW Safety including ‘LDW_Torque_Req’ and ‘activation_status’ shall be protected by an end-to-end (E2E) protection mechanism. | C | E2E calc | LDW_Torq_Req = 0 |
| Software Safety Requirement 02-02 | The E2E protection mechanism shall contain he control data (alive counter and CRC) to the transmitted data. | C | E2E calc | LDW_Torq_Req = 0 |

| ID | Technical Safety Requirement | ASIL | Fault Tolerant Time Interval | Allocation to Architecture | Safe State |
|---|---|---|---|---|---|
| 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 | 50 ms | LDW safety | LDW_Torque_Request is set to zero |

| ID | Software Safety Requirement | ASIL | Allocation Software Elements | Safe State |
|---|---|---|---|---|
| Software Safety Requirement 03-01 | Each software element shall output a signal to indicate an error detected by the element. Error signal = error_status_input (LDW_SAFETY_INPUT_PROCESSING), error_status_torque_limiter(TORQUE_LIMITER), error_status_output_gen(LDW_SAFETY_OUTPUT_GENERATOR) | C | All | N/A |
| Software Safety Requirement 03-02 | Each software element shall evaluate the error status of all other software elements, and in case an error is detected, it shall deactivate LDW (activation_status = 0) | C | LDW_SAFETY_ACTIVATION | LDW function deactivated (activation_status = 0) |
| Software Safety Requirement 03-03 | If no error was detected in any of the software elements, the status of the LDW function shall be set | C | LDW_SAFETY_ACTIVATION | N/A |

| | | | | |
|---|---|---|---|---|
| | to active (activation_status = 1) | | | |
| Software Safety Requirement 03-04 | If an error was detected by any of the software elements, it shall set the value to the corresponding torque to zero, resulting in 'LDW_Torq_Req' also being set to zero | C | All | LDW_Torq_Req=0 |
| Software Safety Requirement 03-05 | If the LDW funciton was deactivated, it will remain in that state until the next ignition cycle (i.e. when the car is turned off and back on) | C | LDW_SAFETY_ACTIVATION | LDW function deactivated (activation_status = 0) |

| ID | Technical Safety Requirement | ASIL | Fault Tolerant Time Interval | Allocation to Architecture | Safe State |
|---|---|---|---|---|---|
| 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 | 50 ms | LDW safety | LDW_Torque_Request is set to zero |

| ID | Software Safety Requirement | ASIL | Allocation Software Elements | Safe State |
|---|---|---|---|---|
| Software Safety Requirement 04-01 | When the LDW function is deactivated (activation_status set to zero), the activation_status shall be sent to the car display ECU. | C | LDW_SAFETY_ACTIVATION, car display ECU | N/A |

| ID | Technical Safety Requirement | ASIL | Fault Tolerant Time Interval | Allocation to Architecture | Safe State |
|---|---|---|---|---|---|
| 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 | Memory check | LDW_Torque_Request is set to zero |

| ID | Software Safety Requirement | ASIL | Allocation Software Elements | Safe State |
|---|---|---|---|---|
| Software Safety Requirement 05-01 | | | | |
| Software Safety Requirement 05-02 | | | | |
| Software Safety Requirement 05-03 | | | | |
| Software Safety Requirement 05-04 | | | | |

# Refined Architecture Diagram