



Elektrobit



UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21



Document history

| Date | Version | Editor | Description |
|------------|---------|-------------|------------------------------|
| 2017/12/10 | 1.0 | Dongmin Kim | First attempt |
| 2018/06/22 | 1.1 | Dongmin Kim | Fixed some error(Safe state) |
| | | | |
| | | | |
| | | | |

Table of Contents

[Document history](#)

[Table of Contents](#)

[Purpose of the Technical Safety Concept](#)

[Inputs to the Technical Safety Concept](#)

[Functional Safety Requirements](#)

[Refined System Architecture from Functional Safety Concept](#)

[Functional overview of architecture elements](#)

[Technical Safety Concept](#)

[Technical Safety Requirements](#)

[Refinement of the System Architecture](#)

[Allocation of Technical Safety Requirements to Architecture Elements](#)

[Warning and Degradation Concept](#)

Purpose of the Technical Safety Concept

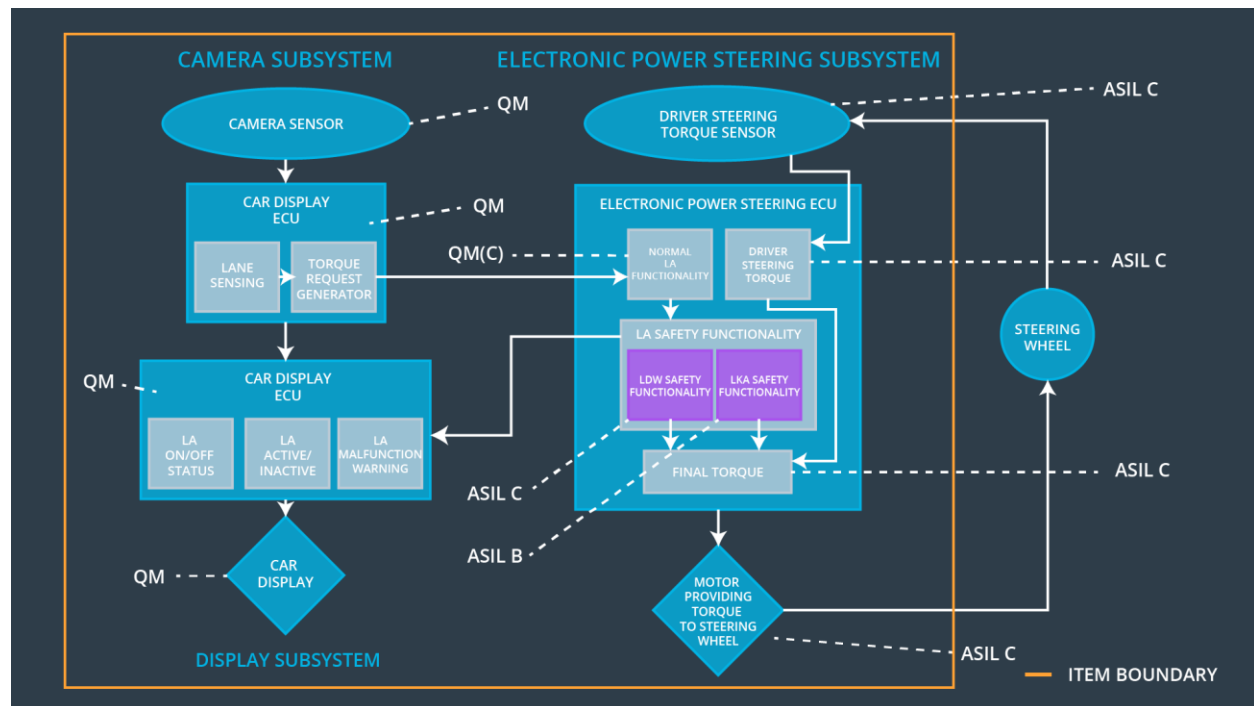
Purpose of the Technical Safety Concept is to turn functional safety requirements into technical safety requirements and to allocate technical safety requirements to the system architecture.

Inputs to the Technical Safety Concept

Functional Safety Requirements

| ID | Functional Safety Requirement | A S I L | Fault Tolerant Time Interval | Safe State |
|--|--|------------------|---------------------------------------|---|
| Functional Safety Requirement 01-01 | The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude. | C | 50ms | LDW is turned off and warning icon is displayed on the car display. |
| Functional Safety Requirement 01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency. | C | 50ms | LDW is turned off and warning icon is displayed on the car display. |
| 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 | LKA is turned off and warning icon is displayed on the car display. |

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

| Element | Description |
|--|---|
| Camera Sensor | The camera sensor reads in images from the road. |
| Camera Sensor ECU - Lane Sensing | The camera sensor ECU is to detect lane lines and determine when the vehicle leaves the lane by mistake. |
| Camera Sensor ECU - Torque request generator | The camera sensor ECU determines the extra torque necessary to steer the vehicle and send request to EPS ECU. |
| Car Display | The car display shows information about lane assistance system. |
| Car Display ECU - Lane Assistance On/Off Status | Car display ECU confirms status about lane assistance On/Off status and send that information to car display. |
| Car Display ECU - Lane Assistant Active/Inactive | Car display ECU confirms status about lane assistance active/inactive and send that information to car display. |

| | |
|--|---|
| Car Display ECU - Lane Assistance malfunction warning | If malfunction is happened, car display ECU send malfunction warning information to car display. |
| Driver Steering Torque Sensor | The driver steering torque sensor is sensing the steering torque. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | EPS ECU get inputs from the driver steering torque sensor, process the data and send that to final torque part. |
| EPS ECU - Normal Lane Assistance Functionality | EPU ECU gets inputs from camera ECU's torque request and sends the output to motor. This torque cannot exceed Max_Torque. |
| EPS ECU - Lane Departure Warning Safety Functionality | EPU ECU assures that the amplitude and frequency do not exceed Max_Torque_Amplitude and Max_Torque_Frequency and sends the output to final torque part. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | EPU ECU assures that the amplitude and frequency do not exceed Max_Duration and sends the output to final torque part. |
| EPS ECU - Final Torque | EPU ECU calculates final torque and sends the output to motor. |
| Motor | The motor provides torque to steering wheel. |

Technical Safety Concept

Technical Safety Requirements

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 | 50 ms | EPS ECU – LDW Safety Functionality | The LDW torque amplitude request 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 | 50 ms | EPS ECU – LDW Safety Functionality | The LDW torque amplitude request 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 | 50 ms | EPS ECU – LDW Safety Functionality | The LDW torque amplitude request 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 | 50 ms | EPS ECU – Data Transmission Integrity Check | The LDW torque amplitude request shall be set to zero |
| 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 – Memory test | The LDW torque amplitude request shall be set to zero |

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 | 50 ms | EPS ECU – LDW Safety Functionality | The LDW torque frequency request 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 | 50 ms | EPS ECU – LDW Safety Functionality | The LDW torque frequency request 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 | 50 ms | EPS ECU – LDW Safety Functionality | The LDW torque frequency request 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 | 50 ms | EPS ECU – Data Transmission Integrity Check | The LDW torque frequency request shall be set to zero display. |

| | | | | | |
|---------------------------------|--|---|----------------|-----------------------|---|
| 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 – Memory test | The LDW torque frequency request shall be set to zero |
|---------------------------------|--|---|----------------|-----------------------|---|

Lane Keeping Assistance (LKA) Requirements:

Functional Safety Requirement 02-1 with its associated system elements
(derived in the functional safety concept)

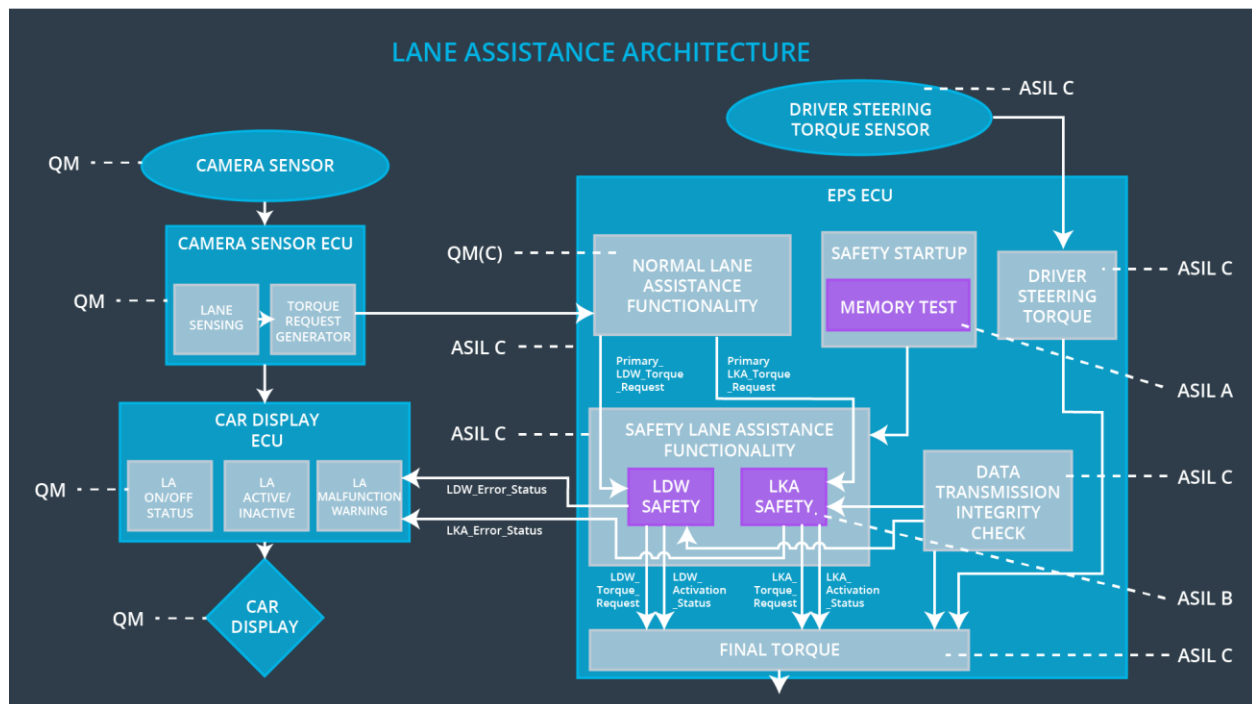
| ID | Functional Safety Requirement | Electronic Power Steering ECU | Camera ECU | Car Display ECU |
|-------------------------------------|---|-------------------------------|------------|-----------------|
| Functional Safety Requirement 02-01 | The lane keeping item shall ensure that the lane keeping 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 that the lane assistance torque is applied for only Max_Duration. | B | 500 ms | EPS ECU – LKA Safety Functionality | LKA is turned off and warning icon is displayed on the car display. |
| 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 warning light. | B | 500 ms | EPS ECU – LKA Safety Functionality | LKA is turned off and warning icon is displayed on the car display. |
| Technical Safety Requirement | As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and | B | 500 ms | EPS ECU – LKA Safety Functionality | LKA is turned off and warning icon is |

| | | | | | |
|---------------------------------|---|---|----------------|---|---|
| 03 | the 'LKA_Torque_Request' shall be set to zero. | | | | displayed on the car display. |
| Technical Safety Requirement 04 | The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured. | B | 500 ms | EPS ECU – Data Transmission Integrity Check | LKA is turned off and warning icon is displayed on the car display. |
| 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 – Memory test | LKA is turned off and warning icon is displayed on the car display. |

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements are allocated to the Electronic Power Steering ECU.

Warning and Degradation Concept

| ID | Degradation Mode | Trigger for Degradation Mode | Safe State invoked? | Driver Warning |
|--------|---|--|---------------------|---|
| WDC-01 | LDW is turned off and warning icon is displayed on the car display. | The LDW torque crosses Max_Torque_Amplitude or Max_Torque_Frequency. | YES | Warning icon is displayed on the car display. |
| WDC-02 | LKA is turned off and warning icon is displayed on the car display. | LKA is activated longer than Max_Duration. | YES | Warning icon is displayed on the car display. |