



Elektrobit



UDACITY

Technical Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21



Document history

| Date | Version | Editor | Description |
|------------|---------|--------|-------------------------------|
| 11/04/2018 | 1.0 | BM | First version of the document |
| | | | |
| | | | |
| | | | |
| | | | |

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

The purpose of the technical safety concept is to further refine the functional safety concept, in a sense that the technical safety concept provides a more detailed description of the technical requirements to achieve functional safety of the product. The technical safety concept assigns

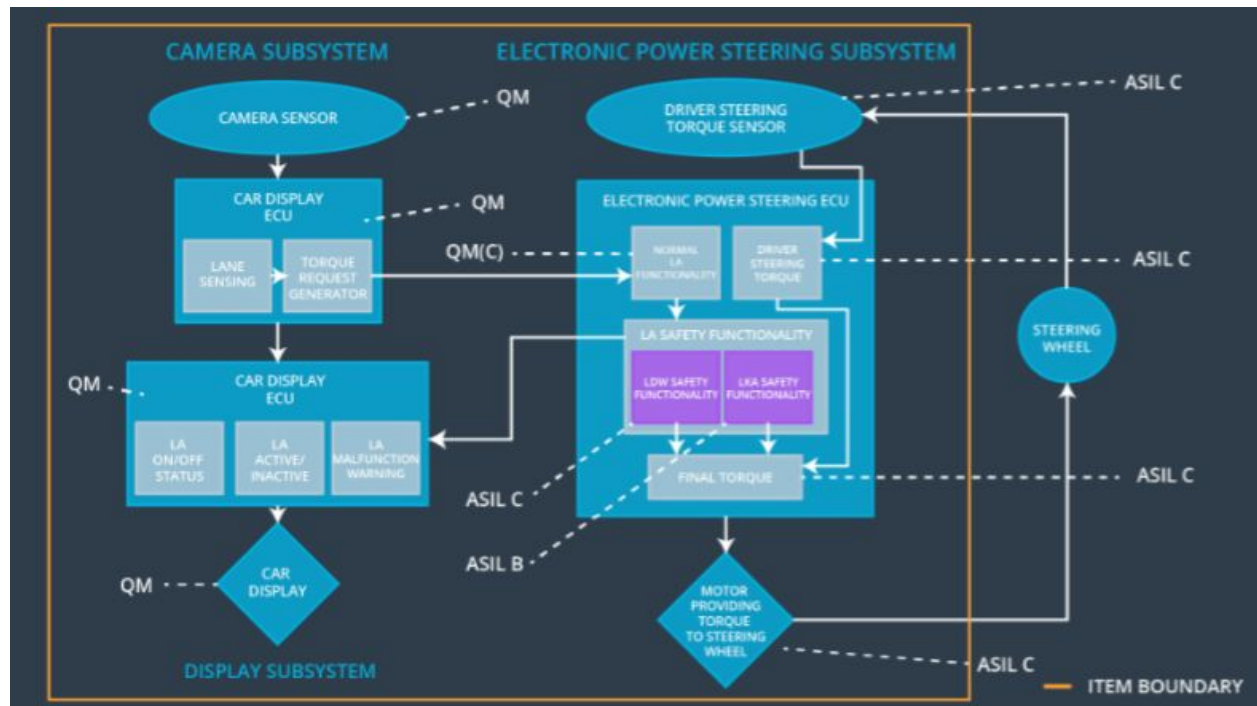
functional safety requirements to the overall system architecture, and as such, the technical safety concept influences software and hardware development directly.

Inputs to the Technical Safety Concept

Functional Safety Requirements

| ID | Functional Safety Requirement | ASIL | Fault Tolerant Time Interval | Safe State |
|-------------------------------------|---|------|------------------------------|--------------------------|
| Functional Safety Requirement 01-01 | Test different values of Max_Torque_Amplitude to ensure that the proper value is chosen for driver's comfort while still preserving meaningful functionality. | C | 50 ms | Function is deactivated. |
| Functional Safety Requirement 01-02 | Test different values of Max_Torque_Frequency to ensure that the proper value is chosen for driver's comfort while still preserving meaningful functionality. | C | 50 ms | Function is deactivated. |
| Functional Safety Requirement 02-01 | The electronic power steering ECU shall ensure that the torque for the Lane Keeping Assistance function is applied for no longer than Max_Duration time interval. | B | 500 ms | Function is deactivated. |

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

| Element | Description |
|--|---|
| Camera Sensor | Provides images to the camera sensor ECU |
| Camera Sensor ECU - Lane Sensing | Calculates the position of the ego vehicle with respect to the center of the ego lane |
| Camera Sensor ECU - Torque request generator | Calculates the necessary torque request based on lane sensing and sends it to the electronic power steering ECU |
| Car Display | Displays information to the driver |
| Car Display ECU - Lane Assistance | Indicates the status of the Lane Assistance |

| | |
|--|---|
| On/Off Status | System (on or off) |
| Car Display ECU - Lane Assistant Active/Inactive | Indicates whether or not the Lane Assistance System is currently active |
| Car Display ECU - Lane Assistance malfunction warning | Turns on in case of the Lane Assistance System malfunction |
| Driver Steering Torque Sensor | Senses the torque that the driver is currently applying to the steering wheel |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Processes the output of the driver steering torque sensor |
| EPS ECU - Normal Lane Assistance Functionality | Software module providing the regular Lane Assistance System functionality |
| EPS ECU - Lane Departure Warning Safety Functionality | Software module ensuring that the torque amplitude and the torque frequency are below the maximum values allowed |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Software module ensuring that the Lane Keeping Assistant function is active not more that the maximum allowed time, to prevent usage as self-driving capability |
| EPS ECU - Final Torque | Software module that generates the final torque value based on the LDW and LKA functions |
| Motor | Applies the final value of the torque to the 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 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 |

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 maximum frequency 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_Frequency” | 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 |

Lane Keeping Assistance (LKA) Requirements:

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

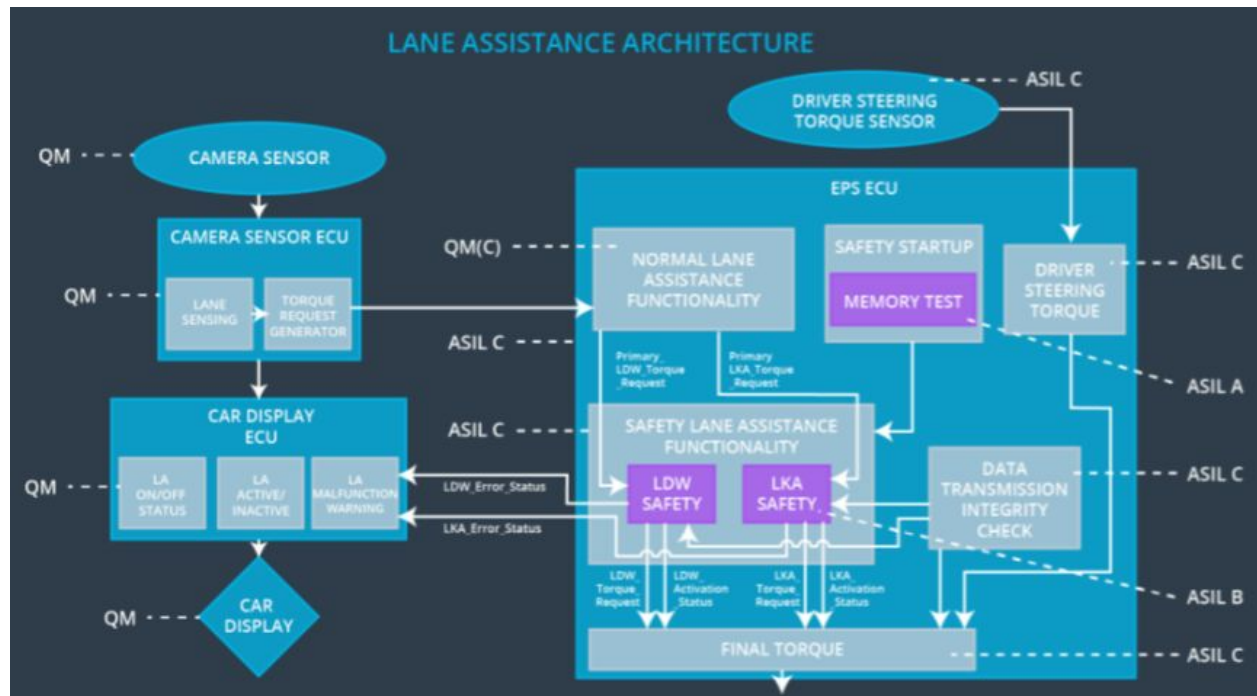
| ID | Functional Safety Requirement | Electronic Power Steering ECU | Camera ECU | Car Display ECU |
|-------------------------------------|---|-------------------------------|------------|-----------------|
| Functional Safety Requirement 02-01 | The lane keeping item shall ensure that the lane keeping 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 duration of the "LKA_Torque_Request" value, which is sent to the "Final electronic power steering Torque" component, is below the maximum allowed value "Max_Duration" | C | 500 ms | LKA safety | LKA_Torque_Request is set to zero |
| Technical Safety Requirement 02 | When the LKA function is deactivated, the LKA safety component shall send a signal to the car display ECU to turn on a warning | C | 500 ms | LKA safety | LKA_Torque_Request is set to zero |

| | | | | | |
|---------------------------------|---|---|----------------|----------------------------------|-----------------------------------|
| | signal. | | | | |
| Technical Safety Requirement 03 | When the LKA safety component detects a failure, it shall deactivate the LKA function and permanently set “LKA_Torque_Request” to zero. | C | 500 ms | LKA safety | LKA_Torque_Request is set to zero |
| Technical Safety Requirement 04 | The validity and integrity of the data transmission for “LKA_Torque_Request” signal shall be ensured. | C | 500 ms | Data transmission integrity test | LKA_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 | LKA_Torque_Request is set to zero |

Refinement of the System Architecture



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

| ID | Degradation Mode | Trigger for Degradation Mode | Safe State invoked? | Driver Warning |
|--------|---------------------------------|------------------------------|---------------------|---|
| WDC-01 | Turn off Lane Assistance System | Malfunction_01 | Yes | Lane Assistance System malfunction warning on car display |

| | | | | |
|--------|---------------------------------|----------------|-----|---|
| WDC-02 | Turn off Lane Assistance System | Malfunction_02 | Yes | Lane Assistance System malfunction warning on car display |
| WDC-03 | Turn off Lane Assistance System | Malfunction_03 | Yes | Lane Assistance System malfunction warning on car display |
| WDC-04 | Turn off Lane Assistance System | Malfunction_04 | Yes | Lane Assistance System malfunction warning on car display |
| WDC-05 | Turn off Lane Assistance System | Malfunction_05 | Yes | Lane Assistance System malfunction warning on car display |