

Functional Safety Concept Lane Assistance

**Document Version: 2.0**

**Released on 2019-06-01**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 01.06.2019 | 1.0 | Sandeep Patil | Initial Version |
| 02.06.2019 | 2.0 | Sandeep Patil | Final Version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[Document history](#_heading=h.3dy6vkm)

[Table of Contents](#_heading=h.4d34og8)

[Purpose of the Functional Safety Concept](#_heading=h.2s8eyo1)

[Inputs to the Functional Safety Analysis](#_heading=h.17dp8vu)

[Safety goals from the Hazard Analysis and Risk Assessment](#_heading=h.3rdcrjn)

[Preliminary Architecture](#_heading=h.26in1rg)

[Description of architecture elements](#_heading=h.lnxbz9)

[Functional Safety Concept](#_heading=h.1y810tw)

[Functional Safety Analysis](#_heading=h.1ksv4uv)

[Functional Safety Requirements](#_heading=h.44sinio)

[Refinement of the System Architecture](#_heading=h.2jxsxqh)

[Allocation of Functional Safety Requirements to Architecture Elements](#_heading=h.z337ya)

[Warning and Degradation Concept](#_heading=h.3j2qqm3)

# Purpose of the Functional Safety Concept

The purpose of functional safety concept is to derive functional safety requirements from functional safety goals. The functional safety requirements thus derived will be high level requirements which will be allocated to different parts of the item architecture. This document also provides the warning and degradation concept

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | The oscillating steering torque from the lane departure warning function shall be limited |
| Safety\_Goal\_02 | The lane keeping assistance function shall be time limited, and the additional steering torque shall end after a given time interval so that the driver cannot misuse the system for autonomous driving |

## Preliminary Architecture

The following figure shows the preliminary architecture for the item LAS



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Capture image of the road and provide it to Camera Sensor ECU |
| Camera Sensor ECU | Detect road lanes and the ego car position in the lane |
| Car Display | Provide feedback to the driver regarding LAS Function enable status and LDW/LKS activation status |
| Car Display ECU | Drive the car display to show the function status and activation information |
| Driver Steering Torque Sensor | Measure the torque applied on steering wheel by driver |
| Electronic Power Steering ECU | Calculate the effective torque to be applied on steering wheel using both torque information from driver and the camera sensor ECU |
| Motor | Apply the final torque calculated by the Electronic Power Steering ECU |

# Functional Safety Concept

The functional safety concept consists of:

* Functional safety analysis
* Functional safety requirements
* Functional safety architecture
* Warning and degradation concept

## Functional Safety Analysis

**[Instructions: Fill in the functional safety analysis table below.]**

|  |  |  |  |
| --- | --- | --- | --- |
| **Malfunction ID** | **Main Function of the Item Related to Safety Goal Violations** | **Guidewords (NO, WRONG, EARLY, LATE, MORE, LESS)** | **Resulting Malfunction** |
| Malfunction\_01 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | MORE | The LDW function shall apply an oscillating steering torque with very high amplitude (above Limit) |
| Malfunction\_02 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | MORE | The LDW function shall apply an oscillating steering torque with very high frequency (above Limit) |
| Malfunction\_03 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | NO | The lane keeping assist is not limited in time which leads to misuse of LKA as autonomous system |

## Functional Safety Requirements

Lane Departure Warning (LDW) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **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 | Vibration torque amplitude < MAX\_TORQUE\_AMPLITUDE |
| 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 | Vibration torque frequency < MAX\_TORQUE\_FREQUENCY |

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

|  |  |  |
| --- | --- | --- |
| **ID** | **Validation Acceptance**  **Criteria and Method** | **Verification Acceptance**  **Criteria and Method** |
| Functional  Safety  Requirement  01-01 | Validate MAX\_TORQUE\_AMPLITUDE chosen is appropriate to be detected by driver and not hindering the steering action | Verify if the system turns off when the amplitude increase more than MAX\_TORQUE\_AMPLITUDE |
| Functional  Safety  Requirement  01-02 | Validate MAX\_TORQUE\_FREQUENCY chosen is appropriate to be detected by driver and not hindering the steering action | Verify if the system turns off when the frequency increase more than MAX\_TORQUE\_FREQUENCY |

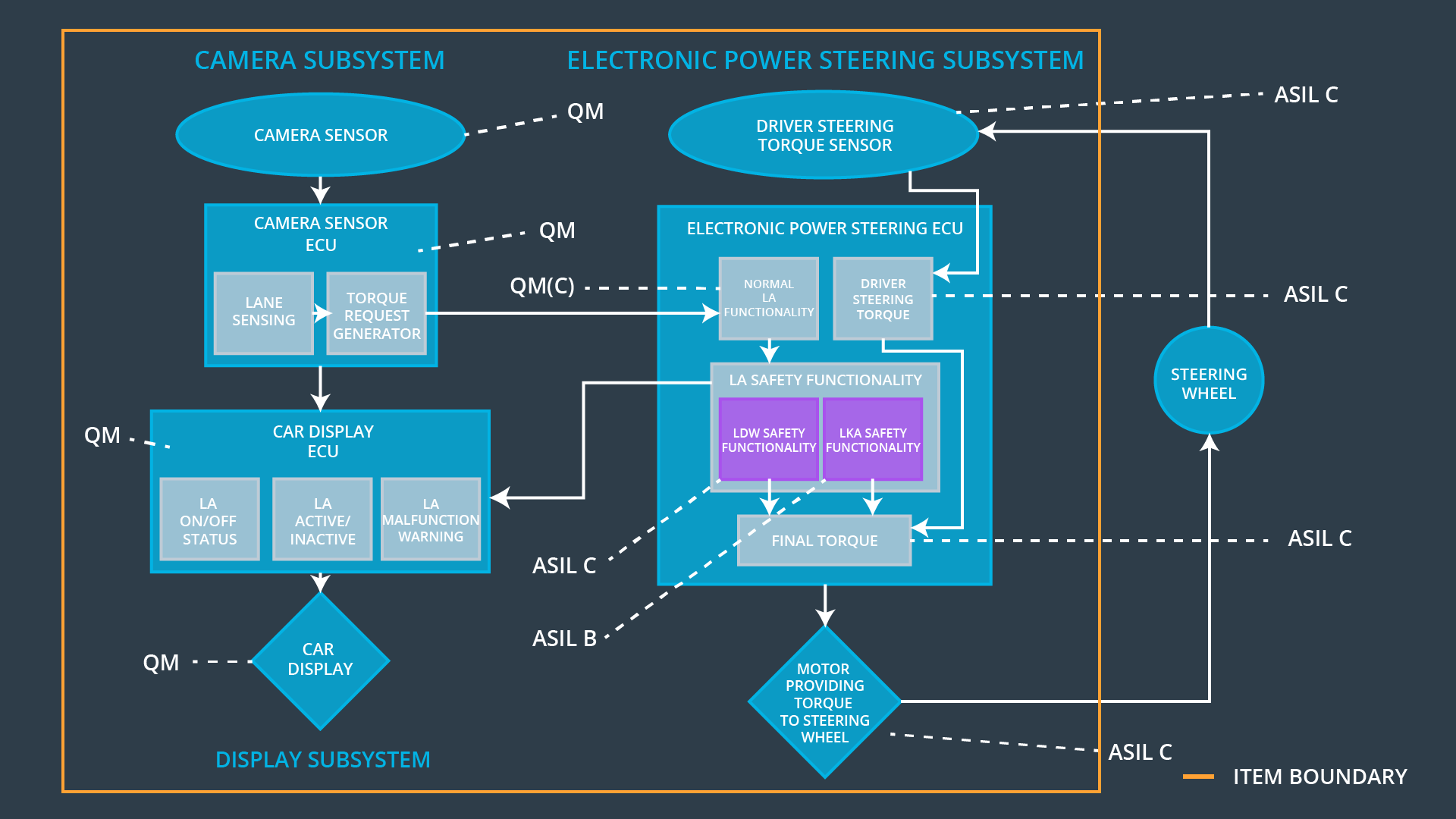
Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  02-01 | The EPS Subsystem shall ensure that the LKA torque is applied only for MAX\_DURATION | C | 500 ms | LKA torque = 0 |

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

|  |  |  |
| --- | --- | --- |
| **ID** | **Validation Acceptance**  **Criteria and Method** | **Verification Acceptance**  **Criteria and Method** |
| Functional  Safety  Requirement  02-01 | Validate MAX\_DURATION is chosen so that the driver cannot use it as self driving car | Verify the system does not deactivate if the LKA torque application exceeds the MAX\_DURATION |

## Refinement of the System Architecture

****

## Allocation of Functional Safety Requirements to Architecture Elements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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** |  |  |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below MAX\_TORQUE\_FREQUENCY | **x** |  |  |
| Functional  Safety  Requirement  02-01 | The EPS Subsystem shall ensure that the LKA torque is applied only for MAX\_DURATION | **x** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off LDW functionality | Malfunction\_01  Malfunction\_02 | Yes | LDW Malfunction warning on display |
| WDC-02 | Turn off LKS functionality | Malfunction\_03 | Yes | LKS Malfunction warning on display |