

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

**Template Version 1.0, Released on 2017-06-21**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 6/18/2019 | 1.0 | Bob Li | Initial version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[Document history](#_Toc11779709)

[Table of Contents](#_Toc11779710)

[Purpose of the Functional Safety Concept](#_Toc11779711)

[Inputs to the Functional Safety Concept](#_Toc11779712)

[Safety goals from the Hazard Analysis and Risk Assessment](#_Toc11779713)

[Preliminary Architecture](#_Toc11779714)

[Description of architecture elements](#_Toc11779715)

[Functional Safety Concept](#_Toc11779716)

[Functional Safety Analysis](#_Toc11779717)

[Functional Safety Requirements](#_Toc11779718)

[Refinement of the System Architecture](#_Toc11779719)

[Allocation of Functional Safety Requirements to Architecture Elements](#_Toc11779720)

[Warning and Degradation Concept](#_Toc11779721)

# Purpose of the Functional Safety Concept

The Functional Safety Concept document the general functionality of the item. The safety goal will be refined and derive the functional safety requirements. These safety requirements are allocated to the relevant parts of the system diagram. Allocation means defining which part of the system architecture will implement each requirement.

# 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



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Capture road images and provide them to the Camera Sensor ECU. |
| Camera Sensor ECU | Analyze the images from Camera Sensor and calculate the car position on the road respect to the road lanes. |
| Car Display | Provide information to the driver by display warnings and status of Lane Assistance System |
| Car Display ECU | Get information from Camera Sensor ECU and control the Car Display to show. |
| Driver Steering Torque Sensor | Measure the Handwheel torque of the driver |
| Electronic Power Steering ECU | Receive the Lane Assistance request from Camera Sensor ECU, receive the handwheel torque from the Driver Steering Torque Sensor. Calculate the steering torque applied by the Motor |
| Motor | Apply the motor torque request from 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

|  |  |  |  |
| --- | --- | --- | --- |
| **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 lane departure warning function applies an oscillating torque with very high torque amplitude |
| Malfunction\_02 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | More | The lane departure warning function applies an oscillating torque with very high torque frequency. |
| Malfunction\_03 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | More | The lane keeping assistance function is not limited in time duration which leads to misuse as an autonomous driving function. |

## 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 EPS ECU shall ensure that the lane departure warning torque amplitude is below Max\_Torque\_Ampliture | C | 50ms | Turn system off |
| Functional  Safety  Requirement  01-02 | The EPS ECU shall ensure that the lane departure warning torque frequency is below Max\_Torque\_Frequency | C | 50ms | Turn system off |

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 | Test and validate that the Max\_Torque\_Amplitude chosen is low enough that the driver does not loss control of the car. | Verify that the system does turn off in time if Max\_Torque\_Amplitude is exceeded. |
| Functional  Safety  Requirement  01-02 | Test and validate that the Max\_Torque\_Frequency chosen is low enough that the drive does not loss control of the car. | Verify that the system does turn off in time if Max\_Torque\_Frequency is exceeded. |

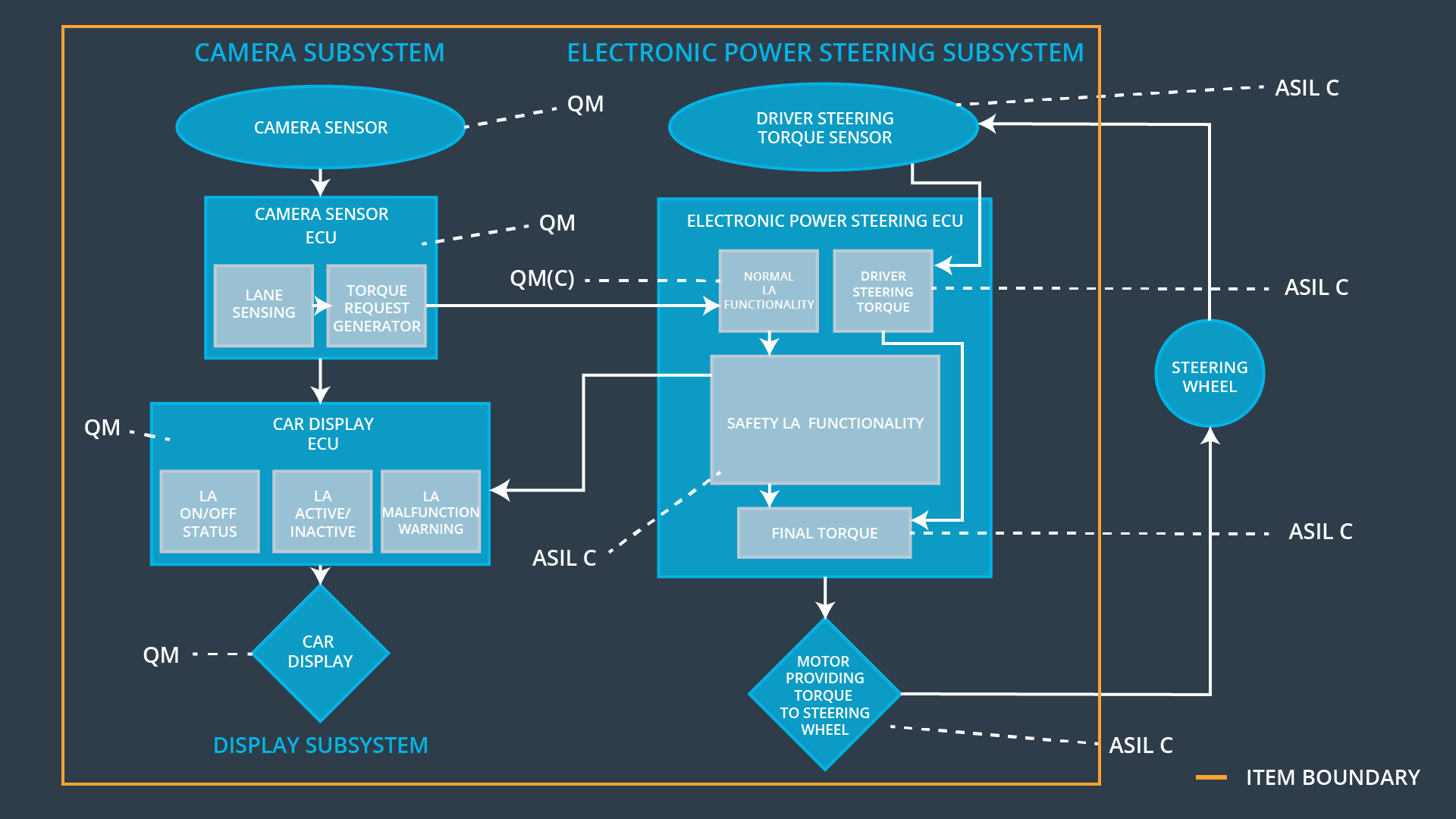
Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  02-01 | The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max-Duration | B | 500ms | Turn system off |

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 | Test and validate that the Max\_Duration chosen really won’t lead driver misuse the LKA function. | Verify that the system does turn off the LKA function if the function activation time is exceeded 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 EPS ECU shall ensure that the lane departure warning torque amplitude is below Max\_Torque\_Ampliture | **√** |  |  |
| Functional  Safety  Requirement  01-02 | The EPS ECU shall ensure that the lane departure warning torque frequency is below Max\_Torque\_Frequency | **√** |  |  |
| Functional  Safety  Requirement  02-01 | The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max-Duration | **√** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn system off | Malfunction\_01  Malfunction\_02 | Yes | Warning light on the car display |
| WDC-02 | Turn system off | Malfunction\_03 | Yes | Warning light on the car display |