

Functional Safety Concept Lane Assistance

**Document Version: 1.0**

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



# 

# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 08.13.2018 | 1.0 | Liang Zhang | First attempt |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[Document history](#_1t3h5sf)

[Table of Contents](#_ktt3lgighckp)

[Purpose of the Functional Safety Concept](#_fulgh8sf1ocg)

[Inputs to the Functional Safety Analysis](#_757cx6xm46zb)

[Safety goals from the Hazard Analysis and Risk Assessment](#_pi1c1upmo8jt)

[Preliminary Architecture](#_s0p6ihti6jgk)

[Description of architecture elements](#_cqb49updinx4)

[Functional Safety Concept](#_mx8us8onanqo)

[Functional Safety Analysis](#_mtn6qbhgsr36)

[Functional Safety Requirements](#_frlc9y84ede8)

[Refinement of the System Architecture](#_74udkdvf7nod)

[Allocation of Functional Safety Requirements to Architecture Elements](#_g2lqf7kmbspk)

[Warning and Degradation Concept](#_4w6r8buy4lrp)

# Purpose of the Functional Safety Concept

Functional safety concept identifies new requirements of the Lane Assistance item and allocate these requirements to system diagrams.

# 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 LDW shall be limited. |
| Safety\_Goal\_02 | The Lane Keeping Assistance function shall be time limited, and additional steering torque shall end after a given time interval so the driver cannot misuse the system for autonomous driving. |

## Preliminary Architecture





### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Send recording images to camera sensor ECU. |
| Camera Sensor ECU | Identify if the vehicle departs from lane. If Yes, send a message to electronic power steering ECU for applying a steering torque. Meantime, send a message to car display ECU for activating lane assistance system. |
| Car Display | Inform driver the status of the lane assistance system and activation/deactivation of the system. Warn drivers if there is a malfunction. |
| Car Display ECU | Identify the status of the lane assistance system, activation/deactivation of the system and if there is a malfunction. |
| Driver Steering Torque Sensor | Measure amplitude, frequency and duration of steering torque from steering wheel and send them to electronic power steering ECU. |
| Electronic Power Steering ECU | Receive messages from camera sensor ECU and measurements from driver steering torque sensor, output torque request to Motor. |
| Motor | Receive torque request from electronic power steering ECU, then provide torque to steering wheel. |

# 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 (above limit) |
| 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 (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 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 lane assistance item shall ensure that the lane departure oscillating torque is below Maximum\_Torque\_Amplitude. | C | 50ms | Turn off LDW component by setting oscillating\_torque to zero |
| Functional  Safety  Requirement  01-02 | The lane assistance item shall ensure that the lane departure oscillating torque is below Maximum\_Torque\_Frequency. | C | 50ms | Turn off LDW component by setting oscillating\_torque to zero |

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 | **Method: test** with how drivers (> 100) react to different torque amplitude.  **Acceptance Criteria**: all the drivers can handle the torque amplitude. | **Method**: software test by inserting a torque amplitude bigger than Maximum\_Torque\_Amplitude.  **Acceptance Criteria**: the lane assistance output is set to zero within the 50 ms fault tolerant time interval. |
| Functional  Safety  Requirement  01-02 | **Method: test** with how drivers (> 100) react to different torque frequency.  **Acceptance Criteria**: all the drivers can handle the torque frequency. | **Method**: software test by inserting a torque amplitude bigger than Maximum\_Torque\_Frequency.  **Acceptance Criteria**: the lane assistance output is set to zero within the 50 ms fault tolerant time interval. |

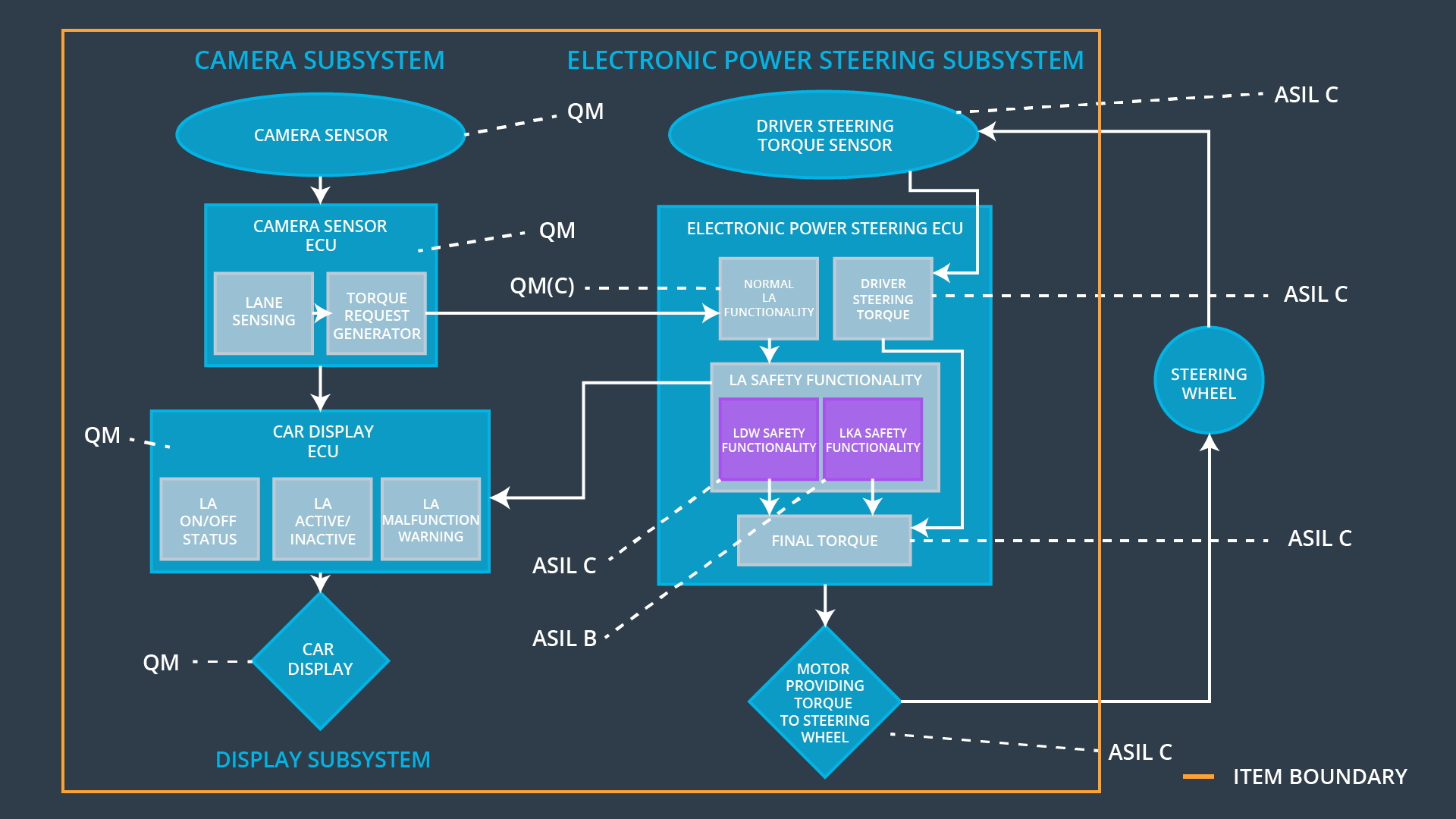
Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  02-01 | The lane assistance item shall ensure that the lane keeping assistance torque is applied for only Max\_Duration. | B | 500 ms | Turn off LKA component by setting steering\_torque to zero. |

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 | **Method: test** with how drivers (> 100) react to different torque duration.  **Acceptance Criteria**: The duration dissuades all drivers from taking their hands off the wheel | **Method**: software test by inserting a torque duration longer than Max\_Duration.  **Acceptance Criteria**: the lane assistance output is set to zero within the 500 ms fault tolerant time interval. |

## 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 electronic power steering ECU shall ensure that the lane departure oscillating torque is below Maximum\_Torque\_Amplitude. | **x** |  |  |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the lane departure oscillating torque is below Maximum\_Torque\_Frequency. | **x** |  |  |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max\_Duration | **x** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turning the lane assistance system off, i.e. the torque request from the lane keeping assistance will be set to zero | The lane departure oscillating torque is above Maximum\_Torque\_Amplitude or Maximum\_Torque\_Frequency | Yes | A warning that the oscillating torque is above the maximum value |
| WDC-02 | Turning the lane assistance system off, i.e. the torque request from the lane keeping assistance will be set to zero | The lane keeping assistance torque is applied longer than Max\_Duration | Yes | A warning that this function is meant for autonomous driving |