

Functional Safety Concept Lane Assistance

**Document Version: 1.0**

**Version 1.0, Released on 2018-04-27**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 04/27/2018 | 1.0 | Ninad Ghike | Initial Creation |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[Document history](#_Toc513106720)

[Table of Contents](#_Toc513106721)

[Purpose of the Functional Safety Concept](#_Toc513106722)

[Inputs to the Functional Safety Concept](#_Toc513106723)

[Safety goals from the Hazard Analysis and Risk Assessment](#_Toc513106724)

[Preliminary Architecture](#_Toc513106725)

[Description of architecture elements](#_Toc513106726)

[Functional Safety Concept](#_Toc513106727)

[Functional Safety Analysis](#_Toc513106728)

[Functional Safety Requirements](#_Toc513106729)

[Refinement of the System Architecture](#_Toc513106730)

[Allocation of Functional Safety Requirements to Architecture Elements](#_Toc513106731)

[Warning and Degradation Concept](#_Toc513106732)

# Purpose of the Functional Safety Concept

The purpose of the Functional Safety Concept is to refine the functional safety goals into functional safety requirements and allocate them to appropriate place in the item architecture.

# 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 LDW function shall be limited |
| Safety\_Goal\_02 | The LKA function shall be time limited and the additional steering torque shall end after a given time interval |

## Preliminary Architecture

The Lane Assistance System architecture is shown in Figure 1.

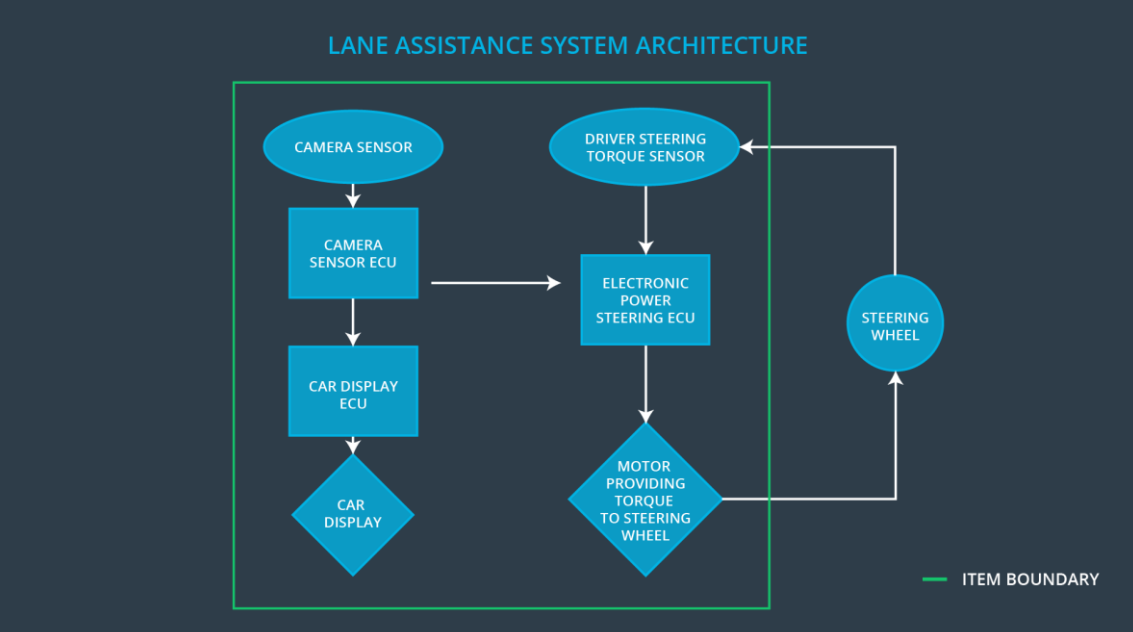


Figure 1

### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | The Camera Sensor reads in images from the road |
| Camera Sensor ECU | The Camera Sensor ECU identifies when the vehicle has accidentally departed its lane, and sends signals to Car Display and torque request to Electronic Power Steering ECU |
| Car Display | The Car Display shows a driver warn signals from Camera Sensor ECU processed by the Car Display ECU |
| Car Display ECU | The Car Display ECU processes signals from the Camera Sensor ECU and sends a signal to the Car Display to turn on/off appropriate status alarm |
| Driver Steering Torque Sensor | The Driver Steering Torque Sensor measures steering torque provided by the driver |
| Electronic Power Steering ECU | The Electronic Power Steering ECU defines the final torque for the Motor |
| Motor | The Motor 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 LDW 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 LDW 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 LKA 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 keeping item shall ensure that the lane departure oscillating torque amplitude is below MAX\_Torque\_Amplitude | C | 50 msec | The LDW torque request shall be set to zero |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below MAX\_Torque\_Frequency | C | 50 msec | The LDW torque request shall be set 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: Testing how drivers react to different vibrational torque amplitudes set for MAX\_Torque\_Amplitude  Acceptance Criteria: All drivers had not difficulty controlling the vehicle because the steering wheel vibration | Method: Software testing. Set vibrational torque amplitudes more than MAX\_Torque\_Amplitude  Acceptance Criteria: The lane assistance system torque output is set to zero within the 50 msec fault tolerant time interval |
| Functional  Safety  Requirement  01-02 | Method: Testing how drivers react to different torque frequency set for MAX\_Torque\_Frequency Acceptance  Criteria: All drivers had not difficulty controlling the vehicle because the steering wheel vibration | Method: Software testing. Set vibrational torque frequency more than MAX\_Torque\_Frequency Acceptance  Criteria: The lane assistance system torque output is set to zero within the 50 msec 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 keeping item shall ensure that the LKA torque is applied for only Max\_Duration | B | 500 msec | The LKA torque request shall be set 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: Testing how drivers react to different duration of the LKA torque request set for Max\_Duration  Acceptance Criteria: No drivers were dissuaded from taking their hands off the wheel | Method: Software testing. Set duration of the LKA torque request more than Max\_Duration  Acceptance Criteria: The lane assistance system torque output is set to zero within the 500 msec fault tolerant time interval |

## Refinement of the System Architecture

Refined system architecture is shown in Figure 2.

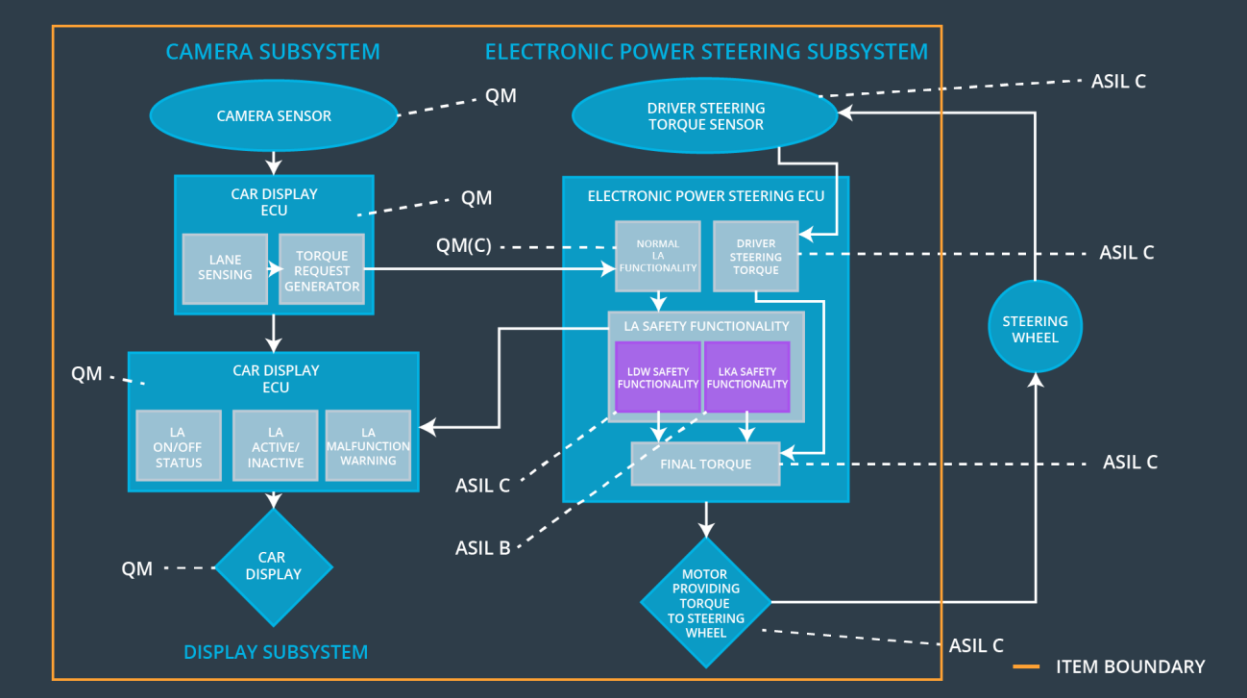


Figure 2

## 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 | **✓** |  |  |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating 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 | Vibrational torque request received by the Electronic Power Steering ECU is very high | Vibrational torque request is higher than MAX\_Torque\_A mplitude or MAX\_Torque\_Fr equency | Yes | Display a malfunction warning light on the driver dashboard |
| WDC-02 | Duration of the LKA torque request received by the electronic power steering ECU is long | Duration of torque request is more than Max\_Duration | Yes | Display a malfunction warning light on the driver dashboard |