

Functional Safety Concept Lane Assistance

**Document Version: 1.0**

**Template Version 2.0, Released on 2017-10-17**



Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2017-10-16 | 1.0 | Daniel Gattringer | Initial version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Document History 2](#_Toc496189089)

[Table of Contents 2](#_Toc496189090)

[1. Purpose of the Functional Safety Concept 3](#_Toc496189091)

[2. Inputs to the Functional Safety Concept 3](#_Toc496189092)

[2.1. Safety goals from the Hazard Analysis and Risk Assessment 3](#_Toc496189093)

[2.2. Preliminary Architecture 3](#_Toc496189094)

[Description of architecture elements 4](#_Toc496189095)

[3. Functional Safety Concept 5](#_Toc496189096)

[3.1. Functional Safety Analysis 5](#_Toc496189097)

[3.2. Functional Safety Requirements 6](#_Toc496189098)

[3.3. Refinement of the System Architecture 7](#_Toc496189099)

[3.4. Allocation of Functional Safety Requirements to Architecture Elements 7](#_Toc496189100)

[3.5. Warning and Degradation Concept 8](#_Toc496189101)

# Purpose of the Functional Safety Concept

The creation of a functional safety concept is part of the safety process of ISO 26262 for the treatment of potential malfunctions in electrical and electronic systems.

From the safety goals, functional safety requirements are derived on system level and assigned to the higher-level 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 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. |
| Safety\_Goal\_03 | The lane departure warning function is designed to prevent it from being activated independently if this is not the intention of the driver. |
| Safety\_Goal\_04 | The lane keeping assistance function shall deactivate itself and shall warn the driver if it is unable to reliably detect lane and road boundaries. |

## Preliminary Architecture

The following image shows the preliminary architecture, which will be refined within this document:



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Sensor for the optical detection of the front area of the vehicle, including detectable lane lines. |
| Camera Sensor ECU | Electronic Control Unit responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake. Responsible for triggering reactions to add extra torque for LDW and LKA functionality. |
| Car Display | Visual display which is, among other functionalities, responsible for displaying warning of lane departures and LKA and LDW activation-status. |
| Car Display ECU | Electronic control unit, which is responsible for creating and providing the data and information that the car display visualizes. |
| Driver Steering Torque Sensor | Sensor responsible for measuring the steering torque provided by the driver. |
| Electronic Power Steering ECU | The electronic control unit is responsible for evaluating the torque provided by the driver and for adding an additional torque based on the torque request of the lane assist system (LKA). Initializes the vibration of the steering wheel when the driver inadvertently drifts away from the center of the lane (LDW). |
| Motor | Mechatronic device which adds extra steering torque directly to the 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  DV04 - Actor effect is too much  (torque amplitude) | 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  DV04 - Actor effect is too much  (torque frequency) | 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  DV03 - Function always activated | The lane keeping assistance function is not limited in time duration which leads to misuse as an autonomous driving function. |
| Malfunction\_04 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | WRONG  DV02 - Function unexpectedly activated | The lane departure warning function is activated independently. The steering wheel begins to oscillate during normal city driving even if the driver expects the system to be deactivated. |
| Malfunction\_05 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | WRONG  DV19 - Sensor detection is wrong | The lane keeping assistance system is activated but the system can't detect the lane boundaries correctly because of snow. The systems interpret the lane boundaries wrong and tries to steer off the road. |

## Functional Safety Requirements

**[Instructions: Fill in the functional safety requirements for the lane departure warning ]**

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 |  |
| 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 |  |
| Functional  Safety  Requirement  01-03 | TODO | A | 50ms |  |

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 |  |  |
| Functional  Safety  Requirement  01-02 |  |  |
| Functional  Safety  Requirement  01-03 |  |  |

**[Instructions: Fill in the functional safety requirements for the lane keeping assistance]**

Lane Keeping Assistance (LKA) Requirements:

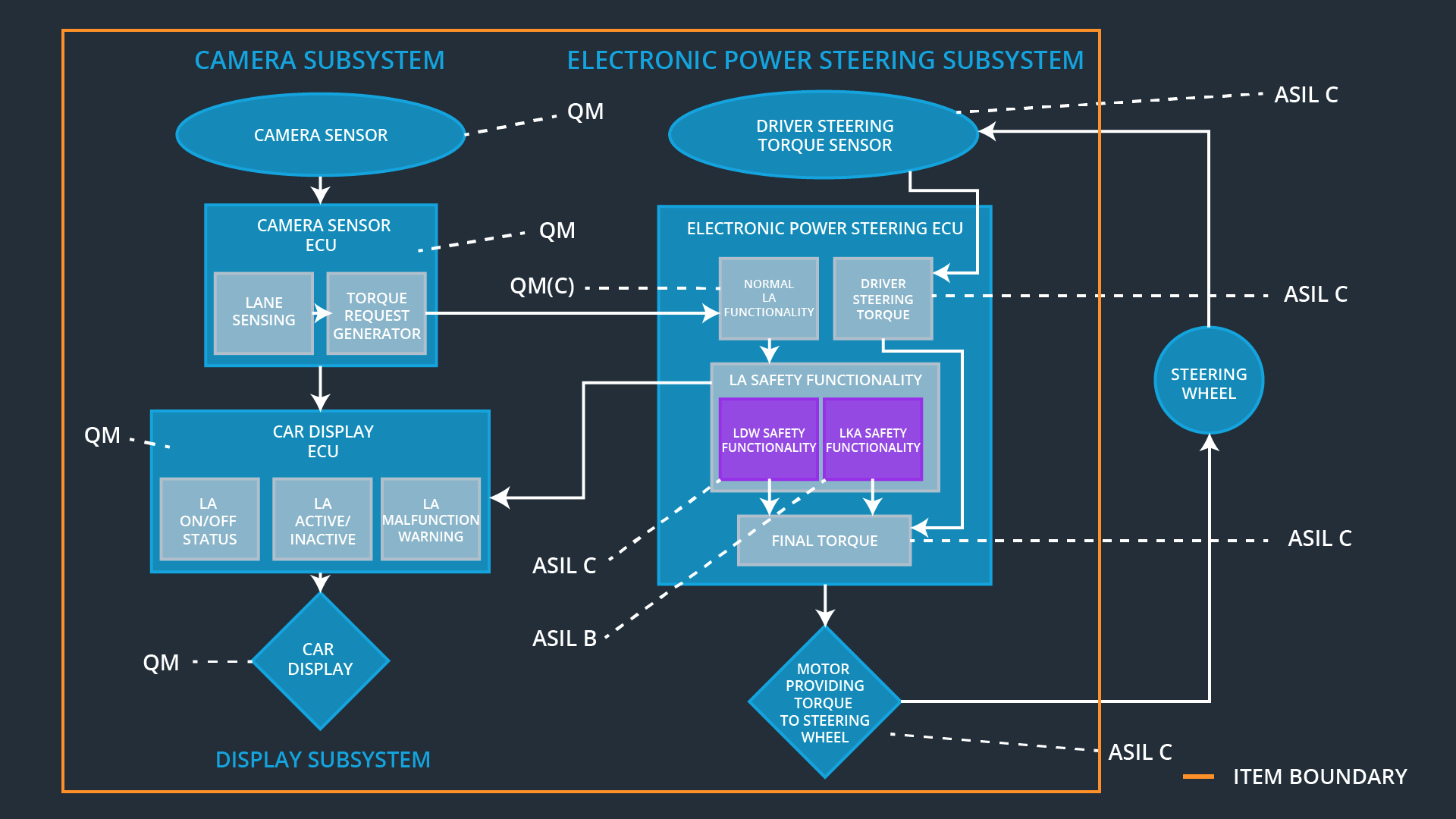
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max\_Duration. | B | 500ms |  |
| Functional  Safety  Requirement  02-02 |  | A | 50ms |  |

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 |  |  |
| Functional  Safety  Requirement  02-02 |  |  |

## Refinement of the System Architecture

The following image shows the refined system architecture:



### Description of architecture elements TODO

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Sensor for the optical detection of the front area of the vehicle, including detectable lane lines. |
| Camera Sensor ECU | Electronic Control Unit responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake. Responsible for triggering reactions to add extra torque for LDW and LKA functionality. |
| Camera Sensor ECU Lane Sensing | Component within the camera sensor ECU responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake. |
| Camera Sensor ECU Torque Request Generator | Component within the camera sensor ECU responsible for calculating and sending an request for additional steering torque for the LDW and LKA functionality. |
| Car Display | Visual display which is, among other functionalities, responsible for displaying warning of lane departures and LKA and LDW activation-status. |
| Car Display ECU | Electronic control unit, which is responsible for creating and providing the data and information that the car display visualizes. |
| Car Display ECU  LA on/off status | Component within the car display ECU responsible for visualizing if the lane assistance functionality is switched on or off. |
| Car Display ECU  LA active/inactive | Component within the car display ECU responsible for visualizing if the lane assistance functionality is active at the moment. Active means the car is drifting away from the center of the lane and LKA is actively acting or the car is getting too narrow to a lane boundary and LDW is warning. |
| Car Display ECU  LA malfunction warning | Component within the car display ECU responsible for visualizing if there occurs any malfunction within the lane assistance system. |
| Driver Steering Torque Sensor | Sensor responsible for measuring the steering torque provided by the driver. |
| Electronic Power Steering (EPS) ECU | The electronic control unit is responsible for evaluating the torque provided by the driver and for adding an additional torque based on the torque request of the lane assist system (LKA). Initializes the vibration of the steering wheel when the driver inadvertently drifts away from the center of the lane (LDW). |
| Motor | Mechatronic device which adds extra steering torque directly to the steering wheel. |

## Allocation of Functional Safety Requirements to Architecture Elements

**[Instructions: Mark which element or elements are responsible for meeting the functional safety requirement. Hint: Only one ECU is responsible for meeting all of the requirements.]**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  01-01 |  |  |  |  |
| Functional  Safety  Requirement  01-02 |  |  |  |  |
| Functional  Safety  Requirement  02-01 |  |  |  |  |

## Warning and Degradation Concept

**[Instructions: Fill in the warning and degradation concept.]**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 |  |  |  |  |
| WDC-02 |  |  |  |  |

# 