

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 01.03.2018 | 1.0 | Qingqing Xia | First version of this document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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

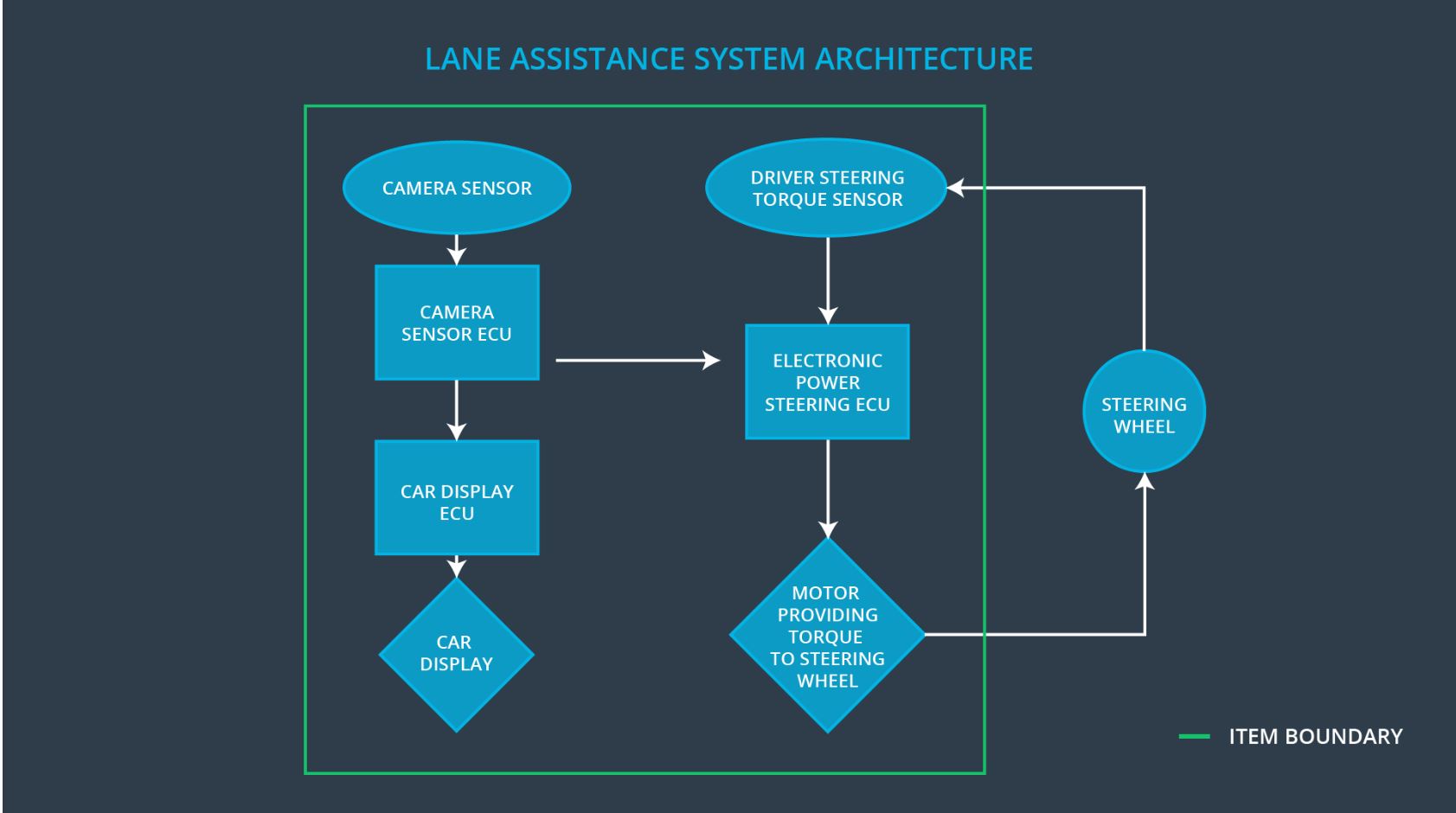
Functional safety concept is looking at the item from a higher level. It looks at the general functionality of the item. In the technical safety concept, it will start looking at different parts of the items, like sensors, control units and actuators. The functional safety concept and technical safety concept are similar in that one will need to identify new requirements 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 the Lane Departure Warning  function 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 | Deliver road images to the Camera Sensor ECU. |
| Camera Sensor ECU | Detects lane lines and determines when the vehicle leaves the lane by mistake. Generates a torque request to the Electronic Power Steering ECU. Triggering the Car Display ECU. |
| Car Display | Show warning to the driver |
| Car Display ECU | Generates warning signals triggered by input from  Camera Sensor ECU and Electronic Power Steering  ECU. |
| Driver Steering Torque Sensor | Measure the steering torque by the driver and provides it to Electronic Power Steering ECU. |
| Electronic Power Steering ECU | Receives the torque by the driver from Driver Steering Torque Sensor and calculates the amount of torque based on Camera Sensor ECU request |
| Motor | Receives torque calculated by Electronic Power  Steering ECU and applies it 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 |
| Malfunction\_04 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | NO | The camera can’t detect the lanes, which lead to uncertain behavior of the LKA. |

## 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 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 | C | 50ms | Vibration frequency is below 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 | To prove we have chosen a Max\_Torque\_Amplitude reasonable value.  We could test how drivers react to different amplitude frequencies to prove that we chose an appropriate value. | When the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval |
| Functional  Safety  Requirement  01-02 | To prove we have chosen a reasonable Max\_Torque\_Frequency value.  We could test how drivers react to different torque frequencies to prove that we chose an appropriate value. | When the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval |

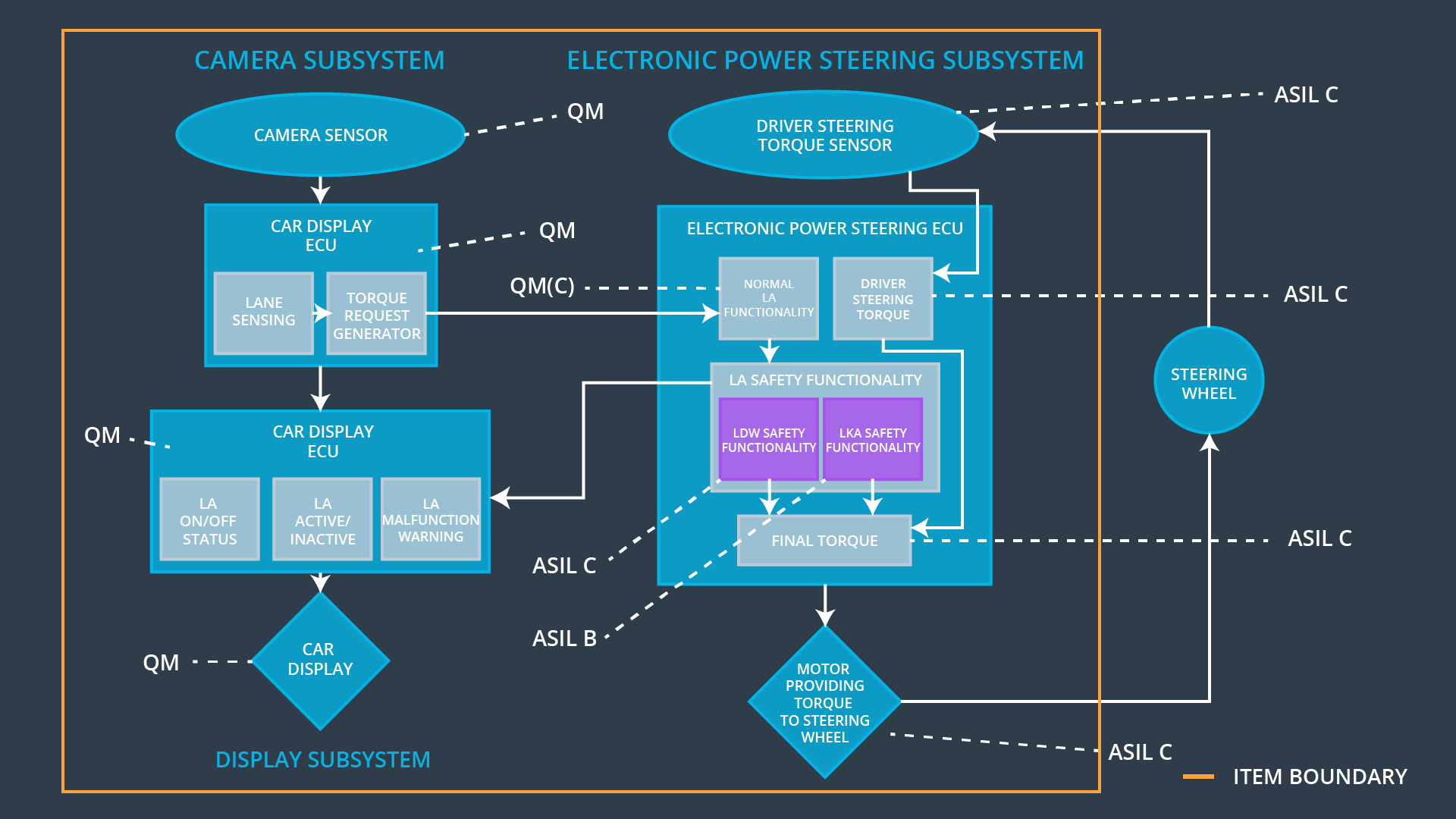
Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU  shall ensure that the Lane Keeping  Assistance torque is applied only  Max\_Duration. | B | 500ms | Lane Keeping  Assistance  torque is zero. |
| Functional  Safety  Requirement  02-02 | The electronic power steering ECU shall  ensure that lane keeping assistance torque zero if camera sensor ECU states Lane\_Not\_Found is true | C | 50ms | Deactive the function |

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 | The max\_duration chosen really did dissuade drivers from taking their hands off the wheel | The system really does turn off if the lane keeping assistance every exceeded max\_duration |
| Functional  Safety  Requirement  02-02 | Validate the Lane Keeping  assistance shall be deactivated  when the camera sensor can’t detect the lane correctly any more. | Verify the system does deactivate the Lane Keeping Assistance if the camera sensor can’t (correctly) detector lanes any more. |

## 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 Departure Warning  item shall ensure that the lane  departure oscillating torque  amplitude is below  Max\_Torque\_Amplitude. | **x** |  |  |
| Functional  Safety  Requirement  01-02 | The Lane Departure Warning  item shall ensure that the lane  departure oscillating torque  frequency is below Max\_Torque\_Frequency. | **x** |  |  |
| Functional  Safety  Requirement  02-01 | The electronic power steering  ECU shall ensure that the lane that the Lane Keeping Assistance torque is applied only Max\_Duration. | **x** |  |  |
| Functional  Safety  Requirement  02-02 | The electronic power steering ECU shall  ensure that lane keeping assistance torqueis zero if camera sensor ECU states Lane\_Not\_Found is true | **x** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off Lane Departure Warning functionality | Malfunction\_01,  Malfunction\_02, | Yes | Lane Departure Warning Malfunction Warning on Car Display |
| WDC-02 | Turn off Lane Keeping Assistance  functionality | Malfunction\_03 | Yes | Lane Keeping Assistance Malfunction Warning on Car Display |