

Technical 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](#_Toc11866657)

[Table of Contents](#_Toc11866658)

[Purpose of the Technical Safety Concept](#_Toc11866659)

[Inputs to the Technical Safety Concept](#_Toc11866660)

[Functional Safety Requirements](#_Toc11866661)

[Refined System Architecture from Functional Safety Concept](#_Toc11866662)

[Functional overview of architecture elements](#_Toc11866663)

[Technical Safety Concept](#_Toc11866664)

[Technical Safety Requirements](#_Toc11866665)

[Refinement of the System Architecture](#_Toc11866666)

[Allocation of Technical Safety Requirements to Architecture Elements](#_Toc11866667)

[Warning and Degradation Concept](#_Toc11866668)

# Purpose of the Technical Safety Concept

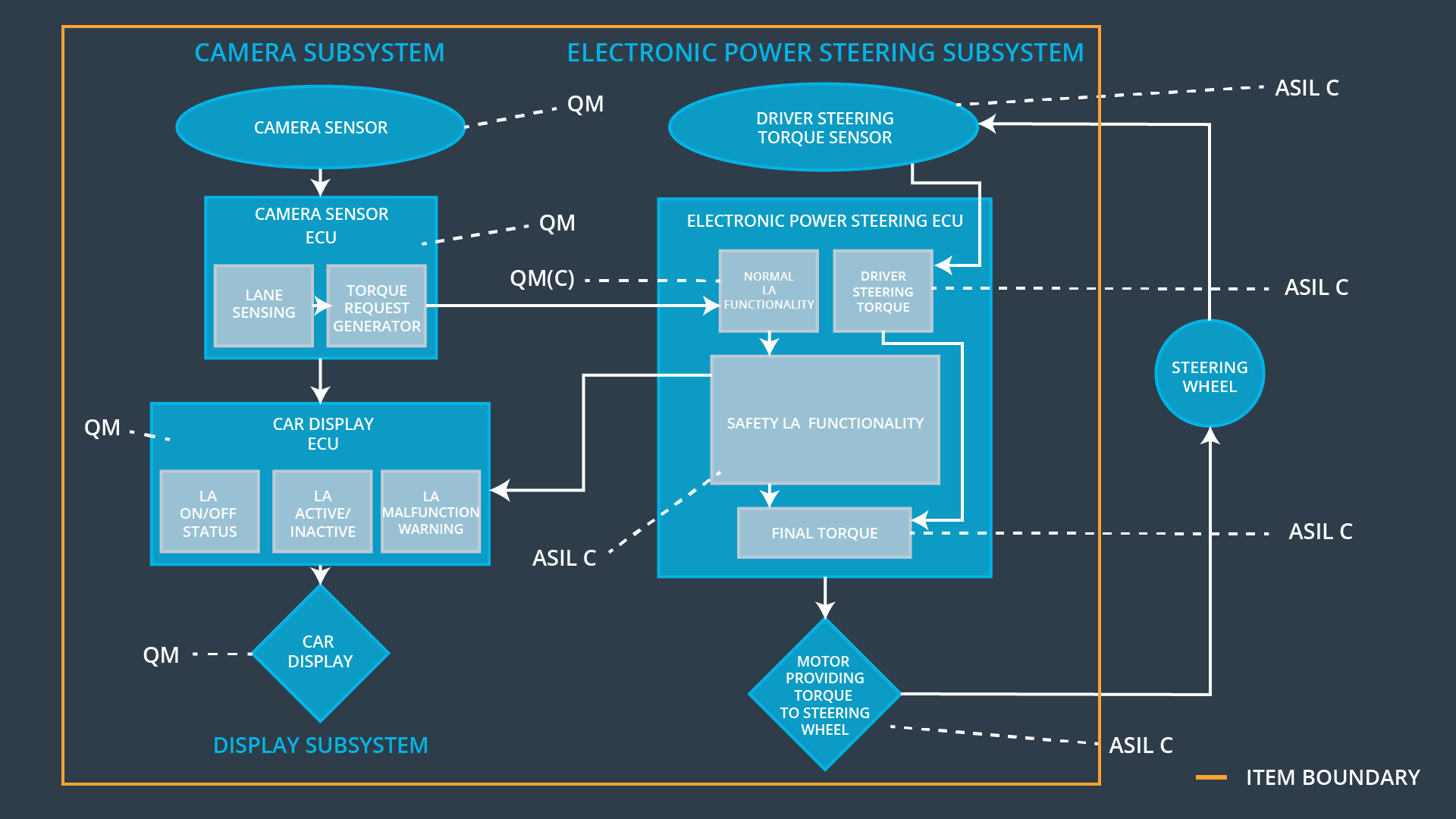
ISO 26262 places the functional safety concept in the concept phase while the technical safety concept is part of the product development phase. Technical safety concept is more concrete and gets into the details of the item's technology.

# Inputs to the Technical Safety Concept

## Functional Safety 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 |
| 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 |

## Refined System Architecture from Functional Safety Concept



### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Capture road images and provide them to the Camera Sensor ECU. |
| Camera Sensor ECU - Lane Sensing | Software module detection the lane line positions from the Camera Sensor images |
| Camera Sensor ECU - Torque request generator | Software module calculation the necessary torque to be requested to the Electronic Power Steering ECU. |
| Car Display | Provide information to the driver by display warnings and status of Lane Assistance System |
| Car Display ECU - Lane Assistance On/Off Status | Indicate the Lane Assistance On/Off Status |
| Car Display ECU - Lane Assistant Active/Inactive | Indicate the Lane Assistant Active/Inactive status |
| Car Display ECU - Lane Assistance malfunction warning | Indicate the Lane Assistance malfunction status |
| Driver Steering Torque Sensor | Measure the Handwheel torque of the driver |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Software module receiving the driver’s torque request from the steering wheel. |
| EPS ECU - Normal Lane Assistance Functionality | Software module receiving the Camera Sensor ECU torque request |
| EPS ECU - Lane Departure Warning Safety Functionality | Software module ensuring the torque amplitude is below Max\_Torque\_Amplitude and torque frequency is below Max\_Torque\_Frequency |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Software module ensuring the Lane Keeping Assistance functionality application is not activate more than Max\_duration time |
| EPS ECU - Final Torque | Combine the torque request from the Lane Keeping and Lane Departure Warning functionalities and sends them to the motor |
| Motor | Apply the motor torque request from the Electronic Power Steering ECU |

# Technical Safety Concept

## Technical Safety Requirements

**Lane Departure Warning (LDW) Requirements:**

Functional Safety Requirement 01-01 with its associated system elements

(derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 | X |  |  |

Technical Safety Requirements related to Functional Safety Requirement 01-01 are:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Architecture Allocation** | **Safe State** |
| Technical  Safety  Requirement  01 | The Lane Departure Warning safety component shall ensure that the amplitude of the ‘LDW\_Torque\_Request’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max\_Torque\_Amplitude.’ | C | 50ms | LDW Safety | Lane Departure Warning torque to zero. |
| Technical  Safety  Requirement  02 | When the Lane Departure Warning is deactivated, the ‘LDW Safety’ software module shall send a signal to the Car Display ECU to turn on a warning signal. | C | 50ms | LDW Safety | Lane Departure Warning torque to zero. |
| Technical  Safety  Requirement  03 | When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set ‘LDW\_Torque\_Request’ to zero. | C | 50ms | LDW Safety | Lane Departure Warning torque to zero. |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for ‘LDW\_Torque\_Request’ signal shall be ensured. | C | 50ms | Data Transmission Integrity Check | Lane Departure Warning torque to zero. |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at start up of the EPS ECU to check for any memory problems | A | Ignition cycle | Safety startup-Memory test | Lane Departure Warning torque to zero. |

Functional Safety Requirement 01-2 with its associated system elements

(derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  01-02 | The EPS ECU shall ensure that the lane departure warning torque frequency is below Max\_Torque\_Frequency | X |  |  |

Technical Safety Requirements related to Functional Safety Requirement 01-02 are:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Architecture Allocation** | **Safe State** |
| Technical  Safety  Requirement  01 | The Lane Departure Warning safety component shall ensure that the frequency of the ‘LDW\_Torque\_Request’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max\_Torque\_Frequency.’ | C | 50ms | LDW Safety | Lane Departure Warning torque to zero. |
| Technical  Safety  Requirement  02 | When the Lane Departure Warning is deactivated, the ‘LDW Safety’ software module shall send a signal to the Car Display ECU to turn on a warning signal. | C | 50ms | LDW Safety | Lane Departure Warning torque to zero. |
| Technical  Safety  Requirement  03 | When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set ‘LDW\_Torque\_Request’ to zero. | C | 50ms | LDW Safety | Lane Departure Warning torque to zero. |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for ‘LDW\_Torque\_Request’ signal shall be ensured. | C | 50ms | Data Transmission Integrity Check | Lane Departure Warning torque to zero. |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at start up of the EPS ECU to check for any memory problems | A | Ignition cycle | Safety startup-Memory test | Lane Departure Warning torque to zero. |

**Lane Keeping Assistance (LKA) Requirements:**

**[Instructions: Fill in the technical safety requirements for the lane keeping assistance functional safety requirement 02-01. We have provided the associated functional safety requirement in the table below. Hint:. You can reuse the technical safety requirements from functional safety requirement 01-01. But you need to change the language because we are now looking at a different system. The ASIL and Fault Tolerant Time Interval are different as well.]**

Functional Safety Requirement 02-1 with its associated system elements

(derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  02-01 | The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max\_Duration | X |  |  |

Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  01 | The Lane Keeping Assistance safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max\_Duration | B | 500ms | LKA Safety | Lane Keeping Assistance torque to zero. |
| Technical  Safety  Requirement  02 | When the Lane Keeping Assistance function deactivates, the ‘LKA Safety’ shall send a signal to the Car Display ECU to turn on a warning light. | B | 500ms | LKA Safety | Lane Keeping Assistance torque to zero. |
| Technical  Safety  Requirement  03 | When a failure is detected, the Lane Keeping Assistance function shall deactivate and the ‘LKA\_Torque\_Request’ shall be zero. | B | 500ms | LKA Safety | Lane Keeping Assistance torque to zero. |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for ‘LKA\_Torque\_Request’ signal shall be ensured. | B | 500ms | Data Transmission Integrity Check | Lane Keeping Assistance torque to zero. |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at start up of the EPS ECU to check for any memory problems | A | Ignition cycle | Safety startup-Memory test | Lane Keeping Assistance torque to zero. |

## Refinement of the System Architecture



## Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements are allocated to the Electronic Power Steering ECU.

## 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 |