

Technical Safety Concept Lane Assistance

**Document Version: 1.0**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2018-10-21 | 1.0 | Rodrigo Vasconcelos | Document creation. |
| 2018-10-22 | 2.0 | Rodrigo Vasconcelos | Adjusted LDW and LKA Safe State to reflect that a better safe state (rather than turning the LA system off) is to set the output torque from the LA functions to zero. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[Document history](#_Toc527918920)

[Table of Contents](#_Toc527918921)

[Purpose of the Technical Safety Concept](#_Toc527918922)

[Inputs to the Technical Safety Concept](#_Toc527918923)

[Functional Safety Requirements](#_Toc527918924)

[Refined System Architecture from Functional Safety Concept](#_Toc527918925)

[Functional overview of architecture elements](#_Toc527918926)

[Technical Safety Concept](#_Toc527918927)

[Technical Safety Requirements](#_Toc527918928)

[Refinement of the System Architecture](#_Toc527918929)

[Allocation of Technical Safety Requirements to Architecture Elements](#_Toc527918930)

[Warning and Degradation Concept](#_Toc527918931)

# Purpose of the Technical Safety Concept

The purpose of this document is to describe what the Lane Assistance item will do when a malfunction violates the safety goal.

# Inputs to the Technical Safety Concept

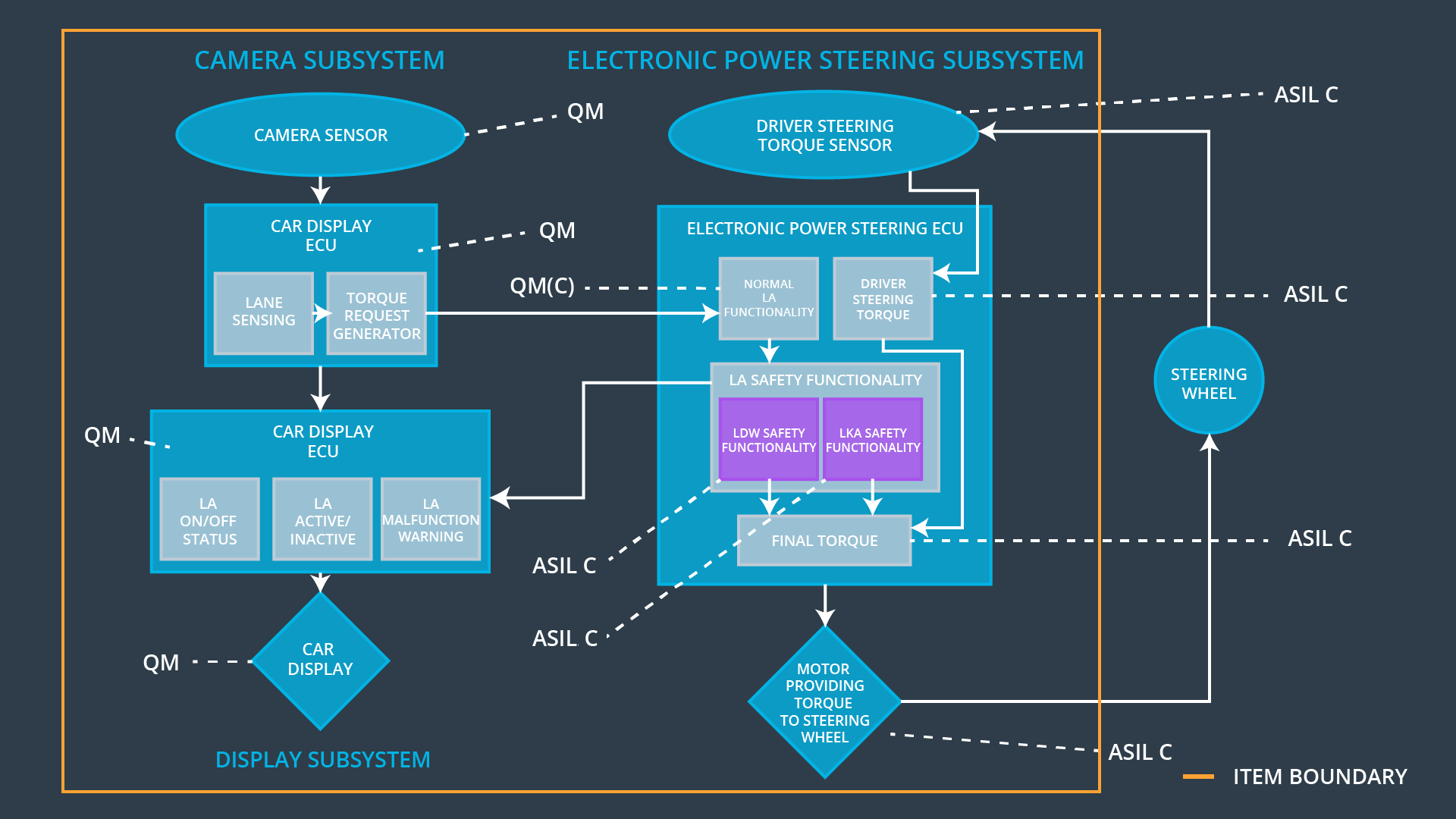
## Functional Safety Requirements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Functional  Safety  Requirement  01-01 | The lane assistance item shall ensure that the lane departure warning oscillating torque amplitude is below Max\_Torque\_Amplitude | C | 50ms | Set LDW output torque to zero |
| Functional  Safety  Requirement  01-02 | The lane assistance item shall ensure that the lane departure warning oscillating torque frequency is below Max\_Torque\_Frequency | C | 50ms | Set LDW output torque to zero |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 | Set LKA output torque to zero |
| Functional  Safety  Requirement  02-02 | The electronic power steering ECU shall ensure that the lane keeping assistance torque applied is not higher than Max\_Torque\_Amount | C | 50ms | Set LKA output torque to zero |

## Refined System Architecture from Functional Safety Concept



### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Capture the scene in front of the car. |
| Camera Sensor ECU - Lane Sensing | Identify lane boundaries and the car’s position relative to the center of the lane. |
| Camera Sensor ECU - Torque request generator | Calculate the torque needed to return the car to the center of the lane. |
| Car Display | Display Lane Assistance system status lights. |
| Car Display ECU - Lane Assistance On/Off Status | Interpret the Lane Assistance system state to activate the “on” light. |
| Car Display ECU - Lane Assistant Active/Inactive | Interpret the Lane Assistance system state to activate the “engaged” light. |
| Car Display ECU - Lane Assistance malfunction warning | Interpret the Lane Assistance system state to activate the “malfunction” light. |
| Driver Steering Torque Sensor | Encode the steering torque applied by the driver. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Record the steering torque applied by the driver. |
| EPS ECU - Normal Lane Assistance Functionality | Request the application of steering torque for lane assistance functions. |
| EPS ECU - Lane Departure Warning Safety Functionality | Ensure that the torque requested by the Normal Lane Assistance Functionality Element is never beyond Max\_Torque\_Amplitude or Max\_Torque\_Frequency |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Ensure that the torque requested by the Lane Assistance Functionality Element is never beyond Max\_Torque\_Magnitude or in excess of Max\_Duration. |
| EPS ECU - Final Torque | Calculates the final torque value from the Lane Assistance Safety Functionality elements and the Driver Steering Torque before sending it to the motor. |
| Motor | Transforms the steering torque commands to actual physical movement of the steering wheel. |

# 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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude | 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 LDW Safety component shall ensure that amplitude of the LDW\_Torque\_Request is below Max\_Torque\_Amplitude | C | 50ms | LDW Safety Element | LDW\_Torque\_Request shall be set to zero |
| Technical  Safety  Requirement  02 | The validity and integrity of the data transmission for the LDW\_Torque\_Request signal shall be ensured. | C | 50ms | Data Transmission Integrity Check | LDW\_Torque\_Request shall be set to zero |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the LDW\_Torque\_Request shall be set to zero. | C | 50ms | LDW Safety Element | LDW\_Torque\_Request shall be set to zero |
| Technical  Safety  Requirement  04 | As soon as the LDW function deactivates the LDW feature, the LDW Safety element shall send a signal to the Car Display ECU to turn on a warning light. | C | 50ms | LDW Safety Element | LDW\_Torque\_Request shall be set to zero |
| Technical  Safety  Requirement  05 | A memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | A | Ignition Cycle | Memory Test | LDW\_Torque\_Request shall be set 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 lane keeping item shall ensure that the lane departure oscillating 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 LDW Safety component shall ensure that frequency of the LDW\_Torque\_Request is below Max\_Torque\_Frequency | C | 50ms | LDW Safety Element | LDW\_Torque\_Request shall be set to zero |
| Technical  Safety  Requirement  02 | The validity and integrity of the data transmission for the LDW\_Torque\_Request signal shall be ensured. | C | 50ms | Data Transmission Integrity Check | LDW\_Torque\_Request shall be set to zero |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the LDW\_Torque\_Request shall be set to zero. | C | 50ms | LDW Safety Element | LDW\_Torque\_Request shall be set to zero |
| Technical  Safety  Requirement  04 | As soon as the LDW function deactivates the LDW feature, the LDW Safety element shall send the LDW\_Error\_Status signal to the Car Display ECU to turn on a warning light. | C | 50ms | LDW Safety Element | LDW\_Torque\_Request shall be set to zero |
| Technical  Safety  Requirement  05 | A memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | A | Ignition Cycle | Memory Test | LDW\_Torque\_Request shall be set to zero |

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

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 LKA Safety component shall ensure that the LKA\_Torque\_Request is only sent for Max\_Duration | C | 500ms | LKA Safety | LKA\_Torque\_Request shall be set to zero |
| Technical  Safety  Requirement  02 | The validity and integrity of the data transmission for the LKA\_Torque\_Request signal shall be ensured. | C | 500ms | Data Transmission Integrity Check | LKA\_Torque\_Request shall be set to zero |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the LKA\_Torque\_Request shall be set to zero. | C | 500ms | LKA Safety | LKA\_Torque\_Request shall be set to zero |
| Technical  Safety  Requirement  04 | As soon as the LKA function deactivates the LKA feature, the LKA Safety element shall send the LKA\_Error\_Status signal to the Car Display ECU to turn on a warning light. | C | 500ms | LKA Safety | LKA\_Torque\_Request shall be set to zero |
| Technical  Safety  Requirement  05 | A memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | A | Ignition Cycle | Memory Test | LKA\_Torque\_Request shall be set to zero |

Functional Safety Requirement 02-2 with its associated system elements

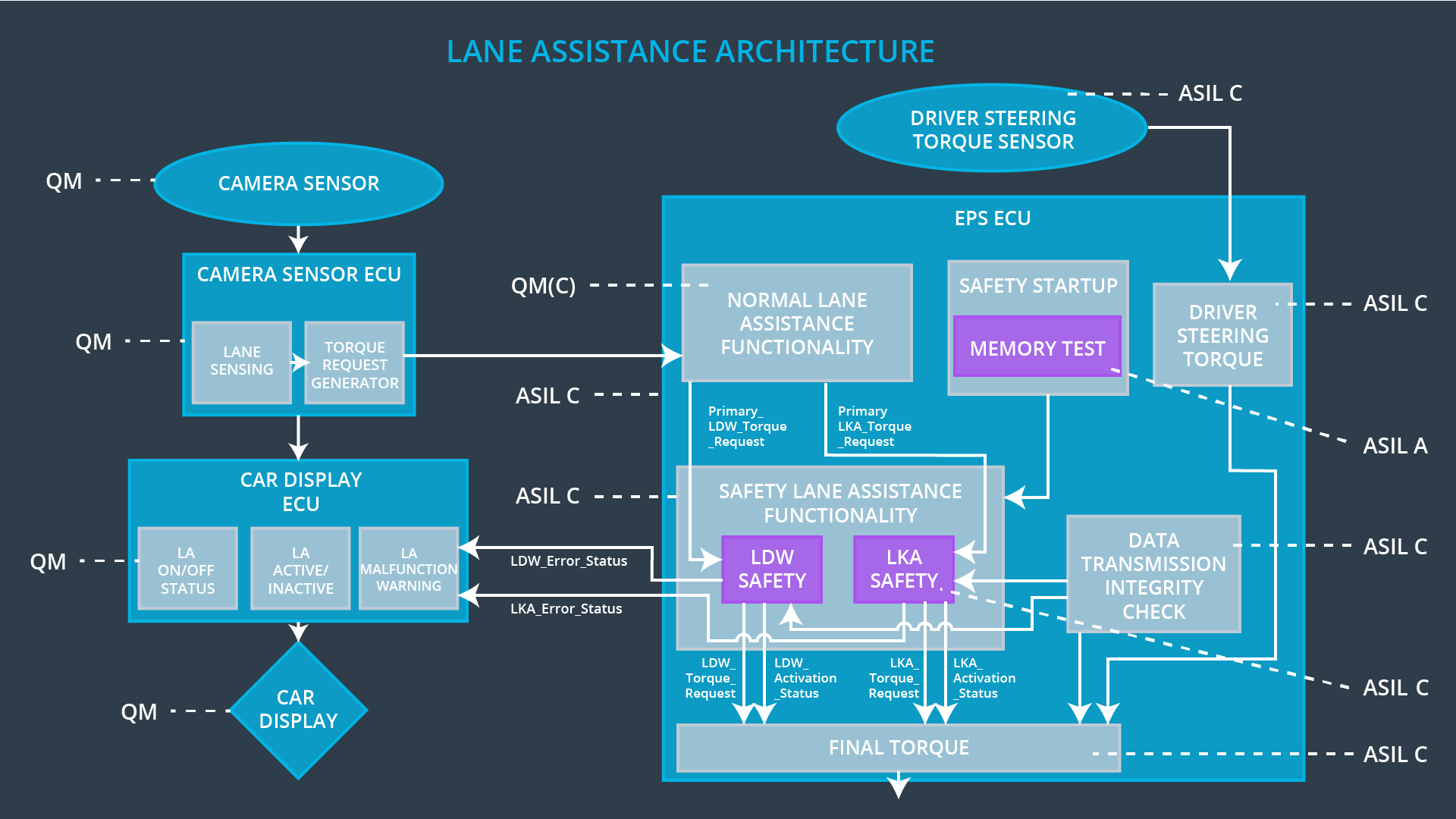
(derived in the functional safety concept)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  02-02 | The electronic power steering ECU shall ensure that the lane keeping assistance torque applied is not higher than Max\_Torque\_Amount | X |  |  |

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  01 | The LKA Safety component shall ensure that amplitude of the LKA\_Torque\_Request is below Max\_Torque\_Amount | C | 50ms | LKA Safety | LKA\_Torque\_Request shall be set to zero |
| Technical  Safety  Requirement  02 | The validity and integrity of the data transmission for the LKA\_Torque\_Request signal shall be ensured. | C | 50ms | Data Transmission Integrity Check | LKA\_Torque\_Request shall be set to zero |
| Technical  Safety  Requirement  03 | As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the LKA\_Torque\_Request shall be set to zero. | C | 50ms | LKA Safety | LKA\_Torque\_Request shall be set to zero |
| Technical  Safety  Requirement  04 | As soon as the LKA function deactivates the LKA feature, the LKA Safety element shall send the LKA\_Error\_Status signal to the Car Display ECU to turn on a warning light. | C | 50ms | LKA Safety | LKA\_Torque\_Request shall be set to zero |
| Technical  Safety  Requirement  05 | A memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | A | Ignition Cycle | Memory Test | LKA\_Torque\_Request shall be set to zero |

## Refinement of the System Architecture



## Allocation of Technical Safety Requirements to Architecture Elements

For the Lane Assistance item, all the technical safety requirements are allocated to the Electronic Power Steering ECU. Specific element allocation is available in the requirement allocation tables.

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off the Lane Assistance item. | Steering oscillating amplitude is too high. | Yes | Display light on dashboard. |
| WDC-02 | Turn off the Lane Assistance item. | Steering oscillating frequency is too high. | Yes | Display light on dashboard. |
| WDC-03 | Turn off the Lane Assistance item. | The lane keeping assistance function is active for more than Max\_Duration. | Yes | Display light on dashboard. |
| WDC-04 | Turn off the Lane Assistance item. | The lane keeping assistance function applies a torque that is too high. | Yes | Display light on dashboard. |