

Technical 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](#_Toc497415696)

[Table of Contents 2](#_Toc497415697)

[1. Purpose of the Technical Safety Concept 3](#_Toc497415698)

[2. Inputs to the Technical Safety Concept 3](#_Toc497415699)

[2.1. Functional Safety Requirements 3](#_Toc497415700)

[2.2. Refined System Architecture from Functional Safety Concept 4](#_Toc497415701)

[3. Technical Safety Concept 6](#_Toc497415702)

[3.1. Technical Safety Requirements 6](#_Toc497415703)

[3.2. Refinement of the System Architecture 12](#_Toc497415704)

[3.3. Allocation of Technical Safety Requirements to Architecture Elements 15](#_Toc497415705)

[3.4. Warning and Degradation Concept 15](#_Toc497415706)

# Purpose of the Technical Safety Concept

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

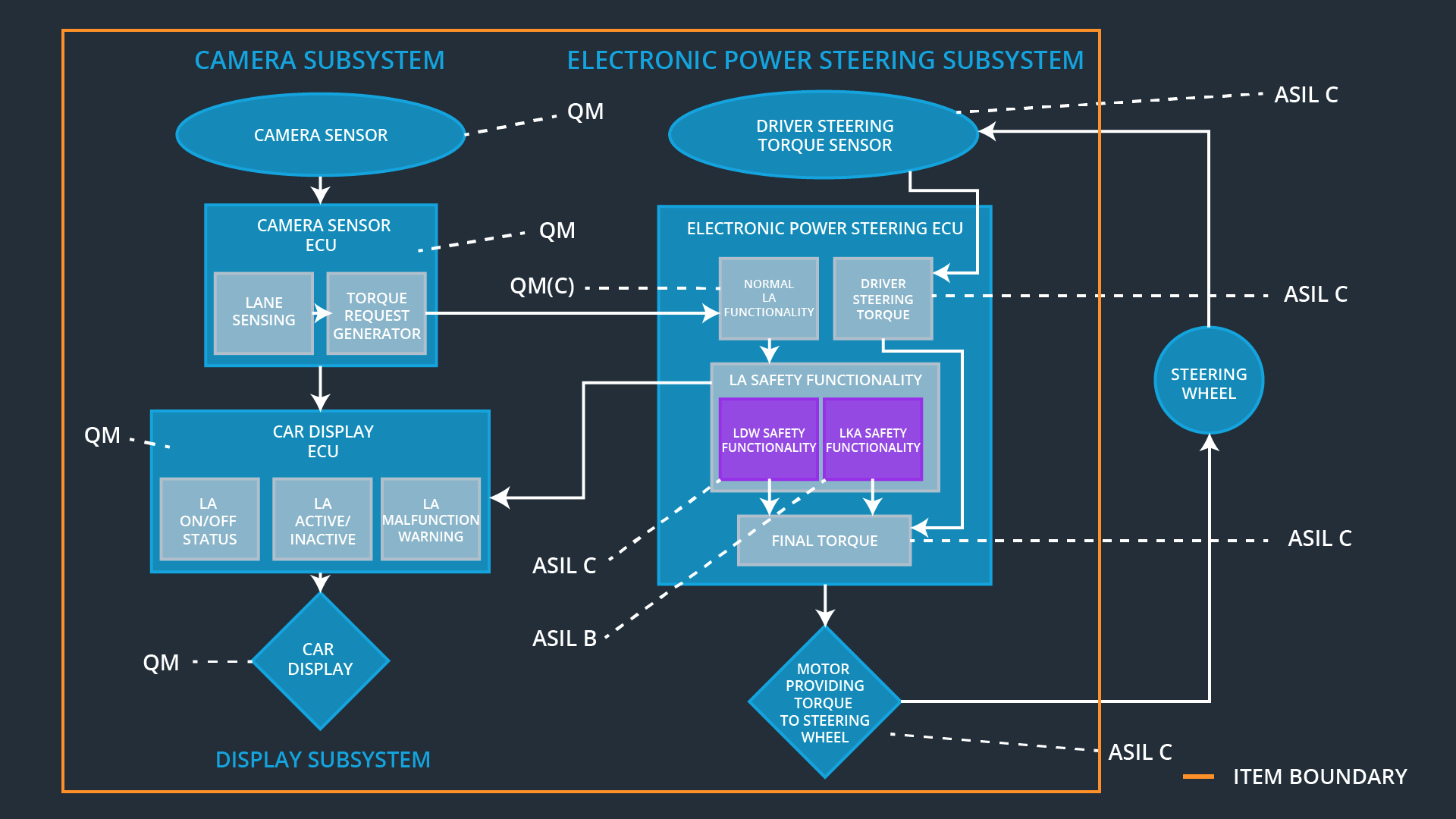
The purpose of the technical safety concept is to transform functional safety requirements to additional technical requirements and allocate these high-level hardware and software requirements to system diagrams of the lane assistance functional safety project.

# 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 keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude. | C | 50ms | Set the oscillating torque 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 | 50ms | Set the oscillating 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 the lane keeping add extra torque to zero. |
| Functional  Safety  Requirement  03-01 | The lane keeping item shall ensure that the lane departure warning by means of vibration of the steering wheel is only possible when LDW\_On is set. | A | 50ms | Set the oscillating torque to zero. |
| Functional  Safety  Requirement  04-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is set to zero when the camera sensor ECU can’t reliably detect the lane boundaries. | A | 50ms | Set the lane keeping add extra torque to zero. |
| Functional  Safety  Requirement  04-02 | The electronic power steering ECU shall ensure that the lane keeping assistance functionality is deactivated and signalized on the car display when the camera sensor ECU can’t reliably detect the lane boundaries. | A | 50ms | Set the lane keeping add extra torque to zero. |

## Refined System Architecture from Functional Safety Concept



Functional overview 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. |
| 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). |
| EPS ECU  Normal Lane Assistance Functionality | Component within the electronic power steering ECU responsible for receiving extra torque request from the camera sensor ECU and doing different non-safety tasks. |
| EPS ECU  Driver Steering Torque | Component within the electronic power steering ECU responsible for receiving the steering torque with which the driver moves the steering wheel. |
| EPS ECU  LDW Safety Functionality | Component within the electronic power steering ECU responsible for keeping the lane departure warning action (oscillating torque) below Max\_Torque\_Amplitude and Max\_Torque\_Frequency.  This component is also responsible for ensuring that the lane departure warning by means of vibration of the steering wheel is only applicated when LDW\_On is set. |
| EPS ECU  LKA Safety Functionality | Component within the electronic power steering ECU responsible for ensuring that the lane keeping assistance is not forcing the car longer than Max\_Duration to the center of the lane.  This component is also responsible for ensuring that the lane keeping assistance by forcing the car to the center of the lane is only applicated when the lane boundaries can be detected reliably. |
| EPS ECU  Final Torque | Component within the electronic power steering ECU responsible for ensuring that the single torque values from LDW, LKA are combined with the drivers original steering torque and sent to the motor. |
| Motor | Mechatronic device which adds extra steering torque directly to 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 |  |  |

The following image shows the LDW safety component of the EPS ECU:



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  01-01-01 | The LDW 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 | EPS ECU -LDW Safety  Component | Set the oscillating torque to zero. |
| Technical  Safety  Requirement  01-01-02 | As soon as the LDW function deactivates the LDW feature, the ‘LDW Safety’ software block shall send a signal to the car display ECU to turn on a warning light. | C | 50ms | EPS ECU -LDW Safety  Component | Set the oscillating torque to zero. |
| Technical  Safety  Requirement  01-01-03 | 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 | EPS ECU -LDW Safety  Component | Set the oscillating torque to zero. |
| Technical  Safety  Requirement  01-01-04 | The validity and integrity of the data transmission for ‘LDW\_Torque\_Request’ signal shall be ensured. | C | 50ms | EPS ECU – Data Transmission Integrity Check | Set the oscillating torque to zero. |
| Technical  Safety  Requirement  01-01-05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | Ignition cycle | EPS ECU –  Safety Startup | Set the oscillating 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 lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency | X |  |  |

The following image shows the LDW safety component of the EPS ECU:



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  01-02-01 | The LDW 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 | EPS ECU -LDW Safety  Component | Set the oscillating torque to zero. |

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

|  |  |  |
| --- | --- | --- |
| **ID** | **Validation Acceptance**  **Criteria and Method** | **Verification Acceptance**  **Criteria and Method** |
| Technical  Safety  Requirement  01-01-01 | Validate that Max\_Torque\_Amplitude is chosen high enough that the driver notices it but low enough not to cause loss of steering. | Verify that the LDW safety component really sets ‘LDW\_Torque\_Request’ to zero if the lane departure warning functionality ever causes a ‘LDW\_Torque\_Request’ with an amplitude above ‘Max\_Torque\_Amplitude’. |
| Technical  Safety  Requirement  01-01-02 | Validate that the warning light for a deactivated LDW feature can be clearly recognized by the driver and is interpreted correctly. | Verify that the LDW safety component really sends a signal to the car display ECU to turn on a warning light every time the LDW function deactivates the LDW feature. |
| Technical  Safety  Requirement  01-01-03 | Validate that the deactivation of the LDW feature and the absence of a vibration warning (in the steering wheel) when leaving the lane will not unsettle the driver and thus distract him. | Verify that the LDW safety component really deactivates the LDW feature and sets the ‘LDW\_Torque\_Request’ to zero every time it detects a failure. |
| Technical  Safety  Requirement  01-01-04 | - | Verify that the Data Transmission Integrity component really checks the validity and integrity of the data transmission for the ‘LDW\_Torque\_Request’ signal every time it is sent. |
| Technical  Safety  Requirement  01-01-05 | - | Verify that the Safety Startup component really checks the memory for any faults every time the EPS ECU is start up. |
| Technical  Safety  Requirement  01-02-01 | Validate that Max\_Torque\_Frequency is chosen high enough that the driver notices it but low enough not to cause loss of steering. | Verify that the LDW safety component really sets ‘LDW\_Torque\_Request’ to zero if the lane departure warning functionality ever causes a ‘LDW\_Torque\_Request’ with an frequency above ‘Max\_Torque\_Frequency. |

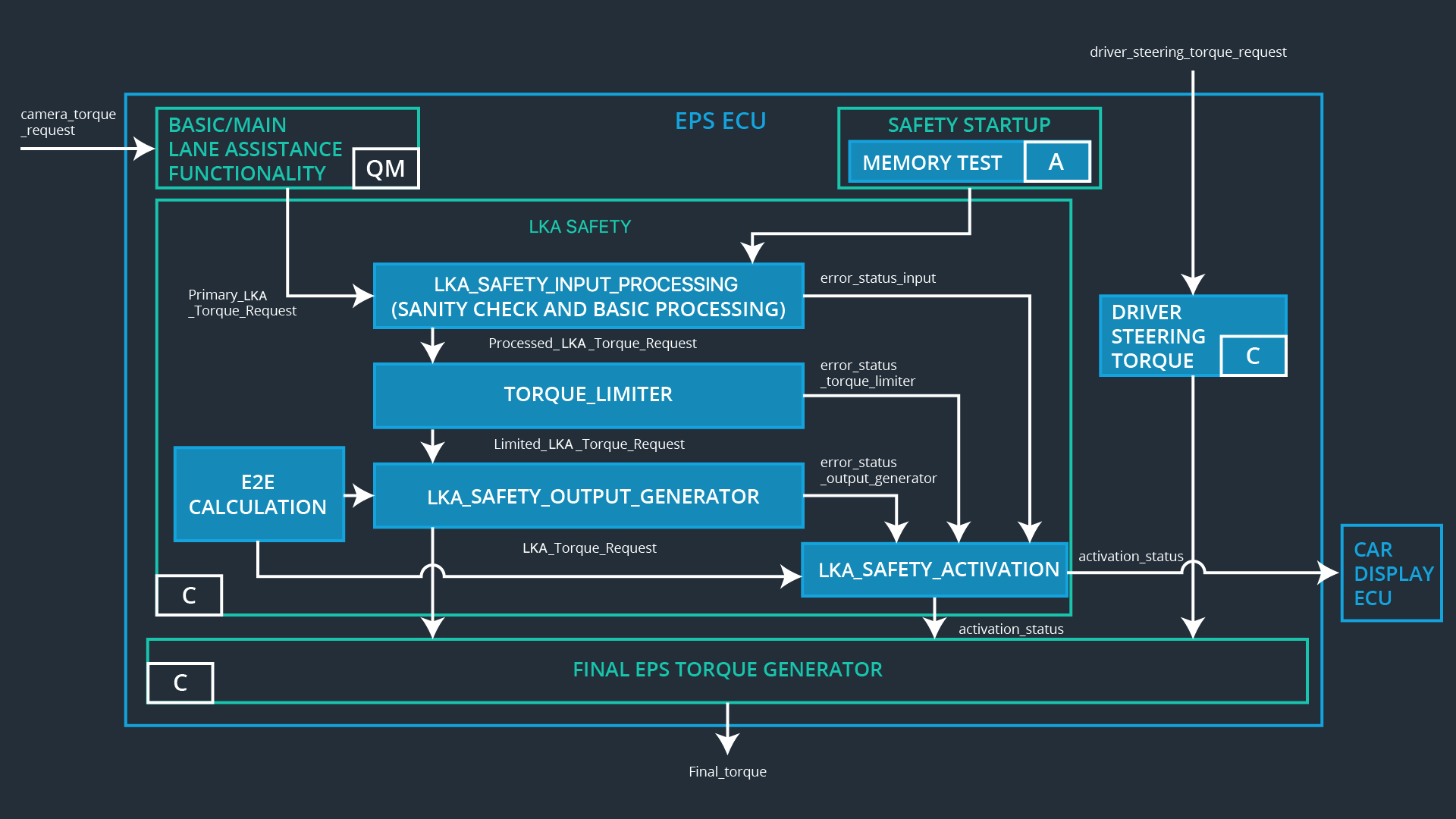
**Lane Keeping Assistance (LKA) Requirements:**

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 duration of the lane keeping assistance torque applied is less than Max\_Duration. | X |  |  |

The following image shows the LKA safety component of the EPS ECU:



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  02-01-01 | The LKA safety component shall ensure that the duration of the lane keeping assistance torque applied is less than Max\_Duration. | C | 500ms | EPS ECU - LKA Safety  Component | Set the lane keeping add extra torque to zero. |
| Technical  Safety  Requirement  02-01-02 | As soon as the LKA function deactivates the LKA feature, the ‘LKA Safety’ software block shall send a signal to the car display ECU to turn on a warning light. | C | 500ms | EPS ECU - LKA Safety  Component | Set the lane keeping add extra torque to zero. |
| Technical  Safety  Requirement  02-01-03 | 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 | EPS ECU - LKA Safety  Component | Set the lane keeping add extra torque to zero. |
| Technical  Safety  Requirement  02-01-04 | The validity and integrity of the data transmission for ‘LKA\_Torque\_Request’ signal shall be ensured. | C | 500ms | EPS ECU – Data Transmission Integrity Check | Set the lane keeping add extra torque to zero. |
| Technical  Safety  Requirement  02-01-05 | Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory. | A | Ignition cycle | EPS ECU –  Safety Startup | Set the lane keeping add extra torque to zero. |

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

|  |  |  |
| --- | --- | --- |
| **ID** | **Validation Acceptance**  **Criteria and Method** | **Verification Acceptance**  **Criteria and Method** |
| Technical  Safety  Requirement  02-01-01 | Validate the allowed usage time of the LKA feature ‘Max\_Duration’ is long enough that it helps the driver to keep within the lane but it is too short to make the driver use the functionality for autonomous driving. | Verify that the LKA safety component really ensures that the LKA feature cannot be used longer than ‘Max\_Duration’, without adding steering torque from the driver. |
| Technical  Safety  Requirement  02-01-02 | Validate that the warning light for a deactivated LKA feature can be clearly recognized by the driver and is interpreted correctly. | Verify that the LKA safety component really sends a signal to the car display ECU to turn on a warning light every time the LKA function deactivates the LKA feature. |
| Technical  Safety  Requirement  02-01-03 | Validate that the deactivation of the LKA feature and the absence of added steering torque when leaving the lane will not unsettle the driver and thus distract him. | Verify that the LKA safety component really deactivates the LKA feature and sets the ‘LKA\_Torque\_Request’ to zero every time it detects a failure. |
| Technical  Safety  Requirement  02-01-04 | - | Verify that the Data Transmission Integrity component really checks the validity and integrity of the data transmission for the ‘LKA\_Torque\_Request’ signal every time it is sent. |
| Technical  Safety  Requirement  02-01-05 | - | Verify that the Safety Startup component really checks the memory for any faults every time the EPS ECU is start up. |

## 

## Refinement of the System Architecture

The following images shows the refined system architecture:

****

Technical overview 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. |
| 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). |
| EPS ECU  Normal Lane Assistance Functionality | Component within the electronic power steering ECU responsible for receiving extra torque request from the camera sensor ECU and doing different non-safety tasks. |
| EPS ECU  Driver Steering Torque | Component within the electronic power steering ECU responsible for receiving the steering torque with which the driver moves the steering wheel. |
| EPS ECU  LDW Safety Functionality | Component within the electronic power steering ECU responsible for keeping the lane departure warning action (oscillating torque) below Max\_Torque\_Amplitude and Max\_Torque\_Frequency.  This component is also responsible for ensuring that the lane departure warning by means of vibration of the steering wheel is only applicated when LDW\_On is set. |
| EPS ECU  LKA Safety Functionality | Component within the electronic power steering ECU responsible for ensuring that the lane keeping assistance is not forcing the car longer than Max\_Duration to the center of the lane.  This component is also responsible for ensuring that the lane keeping assistance by forcing the car to the center of the lane is only applicated when the lane boundaries can be detected reliably. |
| EPS ECU  Final Torque | Component within the electronic power steering ECU responsible for ensuring that the single torque values from LDW, LKA are combined with the drivers original steering torque and sent to the motor. |
| Motor | Mechatronic device which adds extra steering torque directly to the steering wheel. |

## Allocation of Technical Safety Requirements to Architecture Elements

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

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off LDW functionality | Malfunction\_01,  Malfunction\_02,  Malfunction\_04 | Yes, LDW oscillating torque shall be set to zero | Lane assistance functionality set inactive and malfunction warning to the driver via car display. |
| WDC-02 | Turn off LKA functionality | Malfunction\_03,  Malfunction\_05 | Yes, LKA added extra torque shall be set to zero | Lane assistance functionality set inactive and malfunction warning to the driver via car display. |