

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 7/24/2018 | 1.0 | Deepak Zambre | Initial draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[Document history](#_1t3h5sf)

[Table of Contents](#_ktt3lgighckp)

[Purpose of the Technical Safety Concept](#_fulgh8sf1ocg)

[Inputs to the Technical Safety Concept](#_757cx6xm46zb)

[Functional Safety Requirements](#_2f9rjqxbsp2)

[Refined System Architecture from Functional Safety Concept](#_qp3s9pvua9mt)

[Functional overview of architecture elements](#_cqb49updinx4)

[Technical Safety Concept](#_mx8us8onanqo)

[Technical Safety Requirements](#_lnxjuovv6kca)

[Refinement of the System Architecture](#_74udkdvf7nod)

[Allocation of Technical Safety Requirements to Architecture Elements](#_g2lqf7kmbspk)

[Warning and Degradation Concept](#_4w6r8buy4lrp)

# Purpose of the Technical Safety Concept

* Turn functional safety requirements into technical safety requirements
* Allocate technical safety requirements to the system architecture

# 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 land departure oscillating torque amplitude is below MAX\_TORQUE\_AMPLITUDE | C | 50ms | Oscillation torque amplitude less than 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 | Oscillation torque frequency less than MAX\_TORQUE\_FREQUENCY |
| 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 | LKA torque is zero after MAX\_DURATION |

## 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 | To detect lanes from camera images |
| Camera Sensor ECU - Torque request generator | Calculates torque needed to steer car |
| Car Display | Provide​ ​feedback​ ​to​ ​the​ ​driver​ ​displaying​ ​warnings and​ ​the​ ​Lane​ ​Departure​ ​Assistance​ ​status |
| Car Display ECU - Lane Assistance On/Off Status | To tell driver if Lane Assistance is On or Off |
| Car Display ECU - Lane Assistant Active/Inactive | To tell driver if Lane Departure warning is active or inactive |
| Car Display ECU - Lane Assistance malfunction warning | To indicate malfunction in Lane Assistance |
| Driver Steering Torque Sensor | Measure​ ​the​ ​torque​ ​applied​ ​to​ ​the​ ​steering​ ​wheel by​ ​the​ ​driver |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | To sense how much driver is turning the steering wheel |
| EPS ECU - Normal Lane Assistance Functionality | Receives steering torque request from camera subsystem |
| EPS ECU - Lane Departure Warning Safety Functionality | Ensures torque amplitude and frequency are below MAX\_TORQUE\_AMPLITUDE and MAX\_TORQUE\_FREQUENCY respectively |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Ensures LKA is not activated for more than MAX\_DURATION time |
| EPS ECU - Final Torque | Combines torque request from various systems to generate the final torque to be applied |
| Motor | Applies​ ​the​ ​torque​ ​indicated​ ​by​ ​the​ ​Electronic Power​ ​Steering​ ​ECU​ ​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 |  |  |

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 | LDW\_Torque amplitude set to zero. |
| Technical  Safety  Requirement  02 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request’ signal shall be ensured. | C | 50ms | LDW Safety | LDW\_Torque amplitude set to zero. |
| Technical  Safety  Requirement  03 | When 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 | LDW\_Torque amplitude set to zero. |
| Technical  Safety  Requirement  04 | When 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 | LDW Safety | LDW\_Torque amplitude set to zero. |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | A | Ignition cycle | Data Transmission Integrity Check | LDW\_Torque amplitude 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​ ​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 | LDW\_Torque frequency set to zero. |
| Technical  Safety  Requirement  02 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request’ signal shall be ensured. | C | 50ms | LDW Safety | LDW\_Torque frequency set to zero. |
| Technical  Safety  Requirement  03 | When 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 | LDW\_Torque frequency set to zero. |
| Technical  Safety  Requirement  04 | When 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 | LDW Safety | LDW\_Torque frequency set to zero. |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | A | Ignition cycle | Data Transmission Integrity Check | LDW\_Torque frequency set to zero. |

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

**[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]**

**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​ duration​ ​of​ ​the ‘LKA\_Torque\_Request’​ ​is below ‘Max\_Duration.’ | B | 500ms | LKA Safety | LKA\_Torque set to zero. |
| Technical  Safety  Requirement  02 | The validity and integrity of the data transmission for ' LKA\_Torque\_Request’ signal shall be ensured. | B | 500ms | LKA Safety | LKA\_Torque set to zero. |
| Technical  Safety  Requirement  03 | When a failure is detected by the LKA function, it shall deactivate the LKA feature and the 'LKA\_Torque\_Request‘ shall be set to zero. | B | 500ms | LKA Safety | LKA\_Torque set to zero. |
| Technical  Safety  Requirement  04 | When 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. | B | 500ms | LKA Safety | LKA\_Torque set to zero. |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | A | Ignition cycle | Data Transmission Integrity Check | LKA\_Torque set to zero. |

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

**[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]**

## Refinement of the System Architecture

**A screenshot of a video game

Description generated with high confidence**

## Allocation of Technical Safety Requirements to Architecture Elements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Technical  Safety  Requirement  0101-01 | 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.’ | **X** |  |  |
| Technical  Safety  Requirement  0101-02 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request’ signal shall be ensured. | **X** |  |  |
| Technical  Safety  Requirement  0101-03 | When a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW\_Torque\_Request‘ shall be set to zero. | **X** |  |  |
| Technical  Safety  Requirement  0101-04 | When 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. | **X** |  |  |
| Technical  Safety  Requirement  0101-05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | **X** |  |  |
| Technical  Safety  Requirement  0102-01 | 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.’ | **X** |  |  |
| Technical  Safety  Requirement  0102-02 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request’ signal shall be ensured. | **X** |  |  |
| Technical  Safety  Requirement  0102-03 | When a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW\_Torque\_Request‘ shall be set to zero. | **X** |  |  |
| Technical  Safety  Requirement  0102-04 | When 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. | **X** |  |  |
| Technical  Safety  Requirement  0102-05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | **X** |  |  |
| Technical  Safety  Requirement  0201-01 | The​ ​LKA​ ​safety component​ ​shall​ ​ensure that​ ​the​ duration​ ​of​ ​the ‘LKA\_Torque\_Request’​ ​is below ‘Max\_Duration.’ | **X** |  |  |
| Technical  Safety  Requirement  0201-02 | The validity and integrity of the data transmission for ' LKA\_Torque\_Request’ signal shall be ensured. | **X** |  |  |
| Technical  Safety  Requirement  0201-03 | When a failure is detected by the LKA function, it shall deactivate the LKA feature and the 'LKA\_Torque\_Request‘ shall be set to zero. | **X** |  |  |
| Technical  Safety  Requirement  0201-04 | When 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. | **X** |  |  |
| Technical  Safety  Requirement  0201-05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory. | **X** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | turn off the functionality | Malfunction\_01 Malfunction\_02 | Yes | Warning indicator in dashboard |
| WDC-02 | turn off the functionality | Malfunction\_03 | Yes | Warning indicator in dashboard |