

Technical Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 25/08/2017 | 1.0 | Bide Huang | 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

The purpose of the technical safety concept is to identify new requirements and allocate these

high level hardware and software requirements to system diagrams for the lane assistance

functional safety project as pertain to the potential malfunctions of the electrical and electronic

systems as defined by ISO 26262 standard．

# 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 vibration  torque amplitude  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 vibration  torque frequency  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 lane keeping  assistance  torque to zero |

## Refined System Architecture from Functional Safety Concept



### 

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Sensor responsible for capturing vehicle driving  condition including detectable lane lines. |
| Camera Sensor ECU - Lane Sensing | Software Module in 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 | Software Module in the Camera Sensor ECU  responsible for calculating and sending the  additional torque for the LDW and LKA functions. |
| Car Display | Visual display responsible to displaying warning of  lane departures and LKA and LDW activation and  deactivations. |
| Car Display ECU - Lane Assistance On/Off Status | Visual display responsible to displaying LKA and  LDW ON/OFF status. |
| Car Display ECU - Lane Assistant Active/Inactive | Visual display responsible to displaying displaying  warning of lane departures, LKA and LDW  activation and deactivations. |
| Car Display ECU - Lane Assistance malfunction warning | Visual display responsible to displaying warning of  LKA and LDW malfunctions. |
| Driver Steering Torque Sensor | Sensor responsible for measuring how much force  (steering torque) the driver is applying to the  steering wheel. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Software Module in the electronic power steering  ECU responsible for receiving the Camera Sensor  ECU torque requests. |
| EPS ECU - Normal Lane Assistance Functionality | Software Module in the electronic power steering  ECU responsible for receiving the Driver Steering  torque sensor input from the steering wheel. |
| EPS ECU - Lane Departure Warning Safety Functionality | Software Module in the electronic power steering  ECU responsible for keeping the lane departure  oscillating torque amplitude and frequence below  MAX\_Torque\_Amplitude and  MAX\_Torque\_Fequency respectively. |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Software Module in the electronic power steering  ECU responsible for ensuring the application of the  lane keeping assistance torque does not ever  exceeded Max\_Duration and if lane detection is  lost, the LKA function is deactivated. |
| EPS ECU - Final Torque | Software Module in the electronic power steering  ECU responsible for ensuring the LDW, LKA and  the driver’s steering torque requests are combined  and sent to the Motor. |
| Motor | Actuator responsible for applying requested torque  to the steering column by the Electronic Power  Steering ECU for either the LKA or the LDW  functions. |

# Technical Safety Concept

## Technical Safety Requirements

**[Instructions: Fill in the technical safety requirements for the lane departure warning first functional safety requirement. We have provided the associated functional safety requirement in the first table below. Hint: The technical safety requirements were discussed in the lesson videos. The architecture allocation column should contain element names such as LDW Safety block, Data Transmission Integrity Check, etc. Allocating the technical safety requirements to the "EPS ECU" does not provide enough detail for a technical safety concept.]**



**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 the amplitude  of the 'LDW\_Torque\_Request'  sent to the 'Final electronic | C | 50 ms | LDW Safety  block | Set lane  departure  warning  torque to zero |
| Technical  Safety  Requirement  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 | LDW Safety  block | Set lane  departure  warning  torque 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 | 50 ms | LDW Safety  block | Set 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 | LDW Safety  block | Set 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 faults in memory. | A | Ignition  cycle | Data  Transmission  Integrity  Check | Set lane  departure  warning  torque to zero |

**[Instructions: Fill in the technical safety requirements for the lane departure warning second functional safety requirement. We have provided the associated functional safety requirement in the table below. Hint:. Most of the technical safety requirements will be the same. At least one technical safety requirement will have to be slightly modified because we are talking about frequency instead of amplitude. These requirements were not given in the lessons]**

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 the frequency of  "LDW\_Torque\_Request" send to  the "Final electronic power steering  torque" component is below  "Max\_Torque\_Frequency" . | C | 50ms | LDW Safety  Functionallity | LDW  torque  output is  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 | Data  Transmission  integrity check | LDW  torque  output is  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 "LDW\_Torque\_Request" shall be  set to zero. | C | 50ms | LDW Safety  Functionallity | LDW  torque  output is  set to |
| Technical  Safety  Requirement  04 | As soon as the LDW function  deactivates the LDW feature, the  "LDW Safety" software block shall  send a signal to the car display to  turn a warning light. | C | 50ms | LDW Safety  Functionallity | LDW  torque  output is  set to  zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted at  startup of the EPS ECU to check  any faults in memory. | A | Ignition  Cycle | Safety startup  memory test | LDW  torque  output is  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:**

**[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 LKA safety component shall  ensure that the duration of  "LKA\_Torque\_Request" send to  the "Final electronic power  steering torque" component is  below Max\_Duration. | B | 500ms | LKA Safety  Functionallity | LKA torque  output is 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 | Data  Transmission  integrity check | LKA torque  output is 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  "LKA\_Torque\_Request" shall be  set to zero. | B | 500ms | LKA Safety  Functionallity | LKA torque  output is set  to zero |
| Technical  Safety  Requirement  04 | As soon as the LKA function  deactivates the LKA feature, the  "LKA Safety" software block shall  send a signal to the car display to  turn a warning light. | B | 500ms | LKA Safety  Functionallity | LKA torque  output is set  to zero |
| Technical  Safety  Requirement  05 | Memory test shall be conducted  at startup of the EPS ECU to  check any faults in memory. | A | Ignition  Cycle | Safety startup  memory test | LKA torque  output is 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



## Allocation of Technical Safety Requirements to Architecture Elements

**[Instructions: We already included the allocation as part of the technical requirement tables. Here you can state that for this particular item, all technical safety requirements are allocated to the Electronic Power Steering ECU]**

All technical safety requirements for Lane Departure warning and Lane Keeping Assistance 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 off LDW  functionality | Maximum torque  is beyond  Max\_Torque\_A  mplitude | Yes | Car Display |
| WDC-02 | Turn off LKA  functionality | Maximum  duration is  beyond  Max\_Duration | Yes | Car Display |