

Technical Safety Concept Lane Assistance

**Document Version: 1.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 24-May-2018 | 1.0 | Gautam Sareen | Initial Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

Table of Contents

[Document history 2](#_Toc514887349)

[Purpose of the Technical Safety Concept 4](#_Toc514887350)

[Inputs to the Technical Safety Concept 4](#_Toc514887351)

[Functional Safety Requirements 4](#_Toc514887352)

[Refined System Architecture from Functional Safety Concept 4](#_Toc514887353)

[Functional overview of architecture elements 5](#_Toc514887354)

[Technical Safety Concept 6](#_Toc514887355)

[Technical Safety Requirements 6](#_Toc514887356)

[Refinement of the System Architecture 10](#_Toc514887357)

[Allocation of Technical Safety Requirements to Architecture Elements 10](#_Toc514887358)

[Warning and Degradation Concept 10](#_Toc514887359)

# Purpose of the Technical Safety Concept

Technical safety concept is more concrete and gets into the details of the item's technology. Technical safety concept is part of the product development phase. The product development phase also includes designing hardware and software.

# 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 | 50 ms | Turn off  the LDW functionality |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency. | C | 50 ms | Turn off  the LDW functionality |
| Functional  Safety  Requirement  02-01 | Lane keeping assistance Function will be time limited for a Max\_Duration | B | 500ms | Set Lane Keeping Assistance torque to zero and shut off the system |

## Refined System Architecture from Functional Safety Concept



**Fig 1. Lane Assistance System Architecture   
[ image source Udacity course content]**

### Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Captures images and send to camera ECU |
| Camera Sensor ECU - Lane Sensing | Senses the lanes |
| Camera Sensor ECU - Torque request generator | Generate torque request to Electronic Power Steering ECU |
| Car Display | Display status and warnings of the system |
| Car Display ECU - Lane Assistance On/Off Status | Displays whether the lane assistance system is turned on or off. |
| Car Display ECU - Lane Assistant Active/Inactive | Displays whether the Lane Assistance system is active or inactive. |
| Car Display ECU - Lane Assistance malfunction warning | Displays any malfunction or warnings in the Lane Assistance system |
| Driver Steering Torque Sensor | measures torque applied to the steering wheel. |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Processes input from Driver Steering Torque sensor. |
| EPS ECU - Normal Lane Assistance Functionality | It takes input from Driver Steering Torque Sensor and camera ECU and passes it to the safety lane assistance functionality |
| EPS ECU - Lane Departure Warning Safety Functionality | Checks for any malfunction in the Lane Departure Warning function and take appropriate action. (deactivate if there is malfunction, pass the output torque to the final torque is there isn’t any malfunction) |
| EPS ECU - Lane Keeping Assistant Safety Functionality | Checks for any malfunction in the Lane Keeping Assistance function and take appropriate action. (deactivate if there is malfunction, pass the output torque to the final torque is there isn’t any malfunction) |
| EPS ECU - Final Torque | Combine the inputs from LDW , LKA safety functionality and driver steering torque to deliver the final torque request to the motor |
| Motor | Provides torque to steering wheel |

# 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 |  |  |  |  |  |
| Technical  Safety  Requirement  02 |  |  |  |  |  |
| Technical  Safety  Requirement  03 |  |  |  |  |  |
| Technical  Safety  Requirement  04 |  |  |  |  |  |
| Technical  Safety  Requirement  05 |  |  |  |  |  |

**[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 |  |  |  |  |  |
| Technical  Safety  Requirement  02 |  |  |  |  |  |
| Technical  Safety  Requirement  03 |  |  |  |  |  |
| Technical  Safety  Requirement  04 |  |  |  |  |  |
| Technical  Safety  Requirement  05 |  |  |  |  |  |

**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 |  |  |  |  |  |
| Technical  Safety  Requirement  02 |  |  |  |  |  |
| Technical  Safety  Requirement  03 |  |  |  |  |  |
| Technical  Safety  Requirement  04 |  |  |  |  |  |
| Technical  Safety  Requirement  05 |  |  |  |  |  |

**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

**[Instructions: Include the refined system architecture. Hint: The refined system architecture should include the system architecture from the end of the technical safety lesson, including all of the ASIL labels.]**

## 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]**

## Warning and Degradation Concept

**[Instructions: We've already identified that for any system malfunction, the lane assistance functions will be turned off and the driver will receive a warning light indication. The technical safety requirements have not changed how functionality will be degraded or what the warning will be.**

**So in this case, the warning and degradation concept is the same for the technical safety requirements as for the functional safety requirements. You can copy the functional safety warning and degradation concept here.**

**Oftentimes, a technical safety analysis will lead to a more detailed warning and degradation concept. ]**