Elektrobit

UDACITY

# Functional Safety Concept Lane Assistance

**Document Version:** [Version]

Template Version 1.0, Released on 2017-06-21

# Document history

**[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.**

**For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]**

| Date | Version | Editor | Description |
|---|---|---|---|
| 6/21/2018 | 1.0 | Jason Kang | First Deaft |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents

**[Instructions: We have provided a table of contents. If you change the document structure, please update the table of contents accordingly. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In Google Docs, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]**



# Purpose of the Functional Safety Concept

**[Instructions: Answer what is the purpose of a functional safety concept?]**

The goal of this document is to determine which subsystems in the vehicle can be used to meet each functional safety goal. It is meant to discuss implementation from a high level as opposed to the technical details.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

**[Instructions:**
**REQUIRED:**
**Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.**

**OPTIONAL:**
**If you expanded the hazard analysis and risk assessment to include other safety goals, include them here.**
**]**

| ID | Safety Goal |
|---|---|
| Safety_Goal_01 | The oscillating steering torque from the lane departure warning system shall be limited |
| Safety_Goal_02 | The lane keeping assistance function shall be time limited and additional steering torque shall end after given time interval so that the driver cannot misuse the system for autonomous driving |
| Safety_Goal_03 | The maximum time to deliver a warning shall be limited. |
| Safety_Goal_04 | Limit lane keeping assistance shall be disabled under heavy braking conditions. |

# Preliminary Architecture

**[Instructions: Provide a preliminary architecture for the lane assistance item. Hint: See Lesson 3: Item Definition]**

## Description of architecture elements

**[Instructions: Provide a description for each of the item elements; what is each element's purpose in the lane assistance item? ]**

| Element | Description |
|---|---|
| Camera Sensor | Visualizes the road in front of the vehicle. |
| Camera Sensor ECU | Determines the edges of the lane and heading, passes this information to other ECUs. |
| Car Display | Displays warning lights |
| Car Display ECU | Decides which lights to light up on the display based on camera sensor ECU’s data |
| Driver Steering Torque Sensor | Determines the amount of torque the driver is applying to the steering wheel |
| Electronic Power Steering ECU | Figures out how much assisting torque to apply to the steering wheel to help to maintaion lane |
| Motor | Applies additional torque to the steering wheel per direction of the Power Steering ECU |

# Functional Safety Concept

The functional safety concept consists of:

- Functional safety analysis
- Functional safety requirements
- Functional safety architecture
- Warning and degradation concept

## Functional Safety Analysis

**[Instructions: Fill in the functional safety analysis table below.]**

| Malfunction ID | Main Function of the Item Related to Safety Goal Violations | Guidewords (NO, WRONG, EARLY, LATE, MORE, LESS) | Resulting Malfunction |
|---|---|---|---|
| Malfunction_01 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | MORE | "The lane departure warning function applies an oscillating torque with very high torque amplitude (above Max_Torque_Amplitude)" |
| Malfunction_02 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | MORE | "The lane departure warning function applies an oscillating torque with very high torque frequency (above Max_Torque_Frequency)" |
| Malfunction_03 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | NO | "The lane keeping assistance function is not limited in time duration which leads to misuse as an autonomous driving function." |

# Functional Safety Requirements

**[Instructions: Fill in the functional safety requirements for the lane departure warning ]**

Lane Departure Warning (LDW) Requirements:

| ID | Functional Safety Requirement | ASIL | Fault Tolerant Time Interval | Safe State |
|---|---|---|---|---|
| Functional Safety Requirement 01-01 | The power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude | C | 50ms | Set Vibration Torque to 0 |
| Functional Safety Requirement 01-02 | The power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency | C | 50ms | Set Vibration Torque to 0 |

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

| ID | Validation Acceptance Criteria and Method | Verification Acceptance Criteria and Method |
|---|---|---|
| Functional Safety Requirement 01-01 | Test with 20 drivers to make sure that Max_Torque_Amplitude doe not result in lack of control | Use camera ECU to request a torque above Max_Torque_Amplitude. Ensure that Power Steering ECU limits it. |
| Functional Safety Requirement 01-02 | Test with 20 drivers to make sure that Max_Torque_Frequency does not result in lack of control | Use camera ECU to request a torque above Max_Torque_Frequency. Ensure that Power Steering ECU limits it. |

**[Instructions: Fill in the functional safety requirements for the lane keeping assistance]**

Lane Keeping Assistance (LKA) Requirements:

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

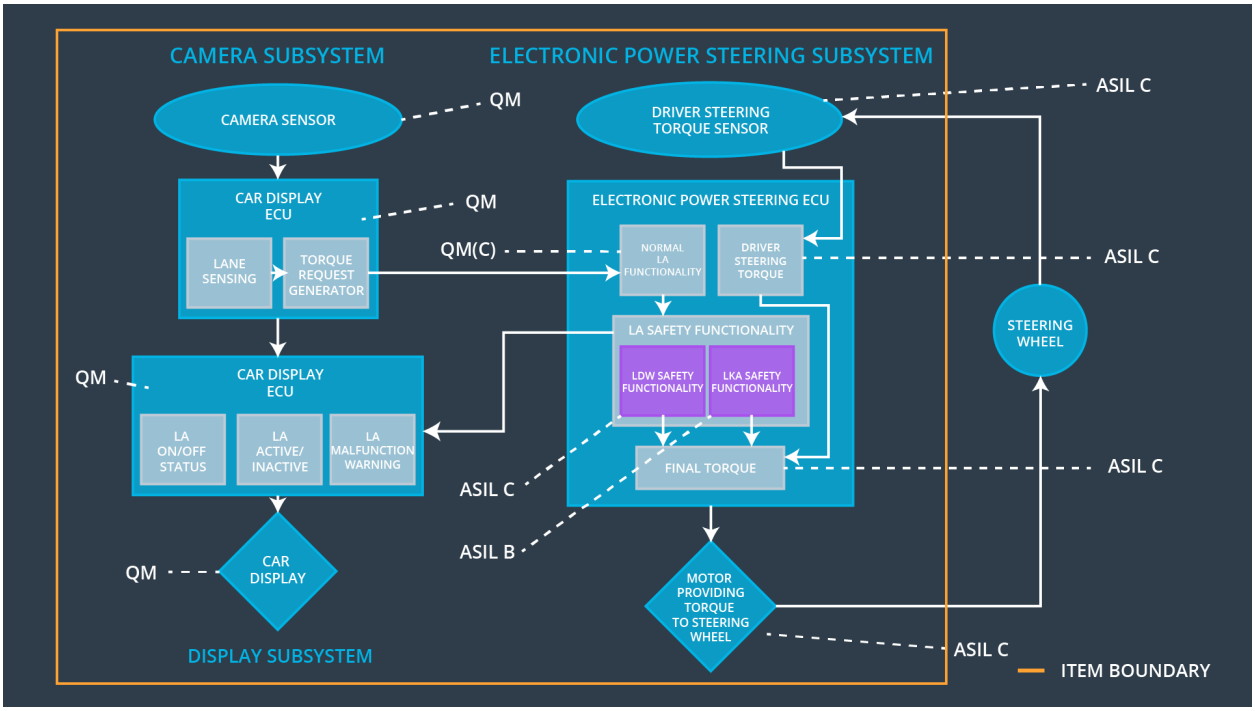
| | | L | Interval | |
|---|---|---|---|---|
| Functional Safety Requirement 02-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration | B | 500ms | lane keeping assistance function disabled |

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

| ID | Validation Acceptance Criteria and Method | Verification Acceptance Criteria and Method |
|---|---|---|
| Functional Safety Requirement 02-01 | Using 20 drivers observe if disabling lane keeping assistance after Max_Duration ms does infact reduce desire to use as self-driving function. | Stray from lane for more than Max_Duration ms. The function should become disabled. |

# 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 functional safety lesson including all of the ASIL labels.]**



## Allocation of Functional Safety Requirements to Architecture Elements

**[Instructions: Mark which element or elements are responsible for meeting the functional safety requirement. Hint: Only one ECU is responsible for meeting all of the requirements.]**

| ID | Functional Safety Requirement | Electronic Power Steering ECU | Camera ECU | Car Display ECU |
|---|---|---|---|---|
| Functional Safety Requirement 01-01 | The power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude | | **x** | |
| Functional Safety Requirement 01-02 | The power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency | | **x** | |
| Functional Safety Requirement 02-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration | | **x** | |

## Warning and Degradation Concept

**[Instructions: Fill in the warning and degradation concept.]**

| ID | Degradation Mode | Trigger for Degradation Mode | Safe State invoked? | Driver Warning |
|---|---|---|---|---|
| WDC-01 | Turn off | Amplitude exceeds Max_Torque_Amplitude or frequency exceeds Max_Torque_Frequency | Yes | Light on Display |
| WDC-02 | Turn off | Torque applied | Yes | Note in user's |

| | | | | |
|---|---|---|---|---|
| | | for longer than Max_Duration | | manual |