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 |
|---|---|---|---|
| 2017-09-17 | 1.0 | Sundeep Tuteja | Functional Safety Concept |
| | | | |
| | | | |
| | | | |
| | | | |

# 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 purpose of a functional safety concept is to refine the safety goals obtained from the Hazard Analysis and Risk Assessment document (HARA) into functional safety requirements, which have the following attributes:

- The ASIL level
- The fault tolerant time interval, which measures how quickly a system needs to react ot a hazardous situation
- The safe state, which discusses what a system looks like after it has avoided an accident

The functional safety concept is also required to allocate these safety requirements to the relevant parts of the system diagram, i.e., define which part of the system architecture will implement each requirement.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

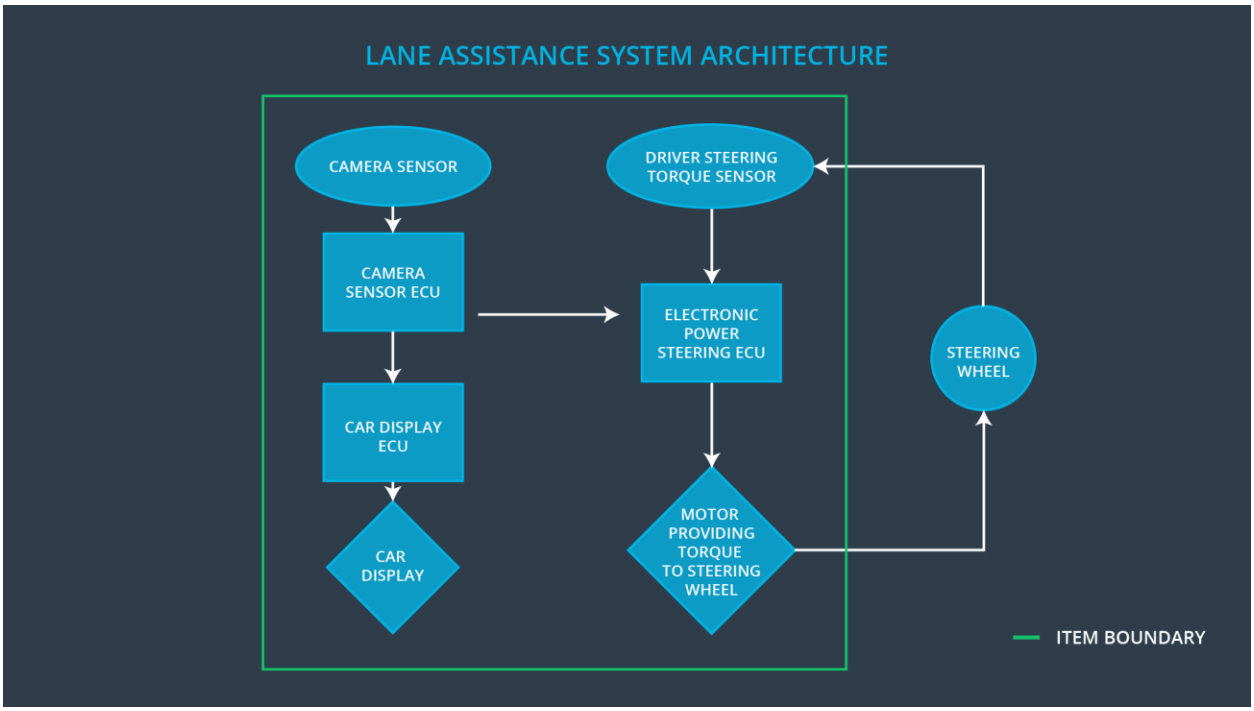
**[Instructions:**
**REQUIRED:**
**Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.**

**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 lane departure warning function should limit the torque applied to the steering wheel to an acceptable upper limit |
| Safety_Goal_02 | The lane keeping assistance function should not always be activated. It should be time limited so that it cannot be misused. |

# 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 | The camera sensor captures images from the road |
| Camera Sensor ECU | The camera sensor ECU identifies situations when the vehicle has unintentionally crossed its lane and communicates a corresponding message to the Car Display ECU and the Electronic Power Steering ECU |
| Car Display | The Car Display displays information about lane assistance system activity to the driver |
| Car Display ECU | The Car Display ECU reads messages from the Camera Sensor ECU about whether the vehicle has unintentionally crossed its lane, and relays the appropriate information to the Car Display |
| Driver Steering Torque Sensor | The driver steering torque sensor reads the torque |

| | |
|---|---|
| | applied to the steering wheel |
| Electronic Power Steering ECU | The electronic power steering ECU reads information from the driver steering torque sensor and the camera sensor ECU, and computes the appropriate amount of torque to be applied to the steering wheel |
| Motor | The motor reads in the torque value to be applied to the steering wheel, and applies it |

# 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 limit) |
| 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 limit) |
| Malfunction_03 | Lane Keeping | NO | The lane keeping |

| | | | |
|---|---|---|---|
| | Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | | 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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude | C | 50 ms | The lane keeping item shall be disabled, output should be 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 | 50 ms | The lane keeping item shall be disabled, output should be zero |

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 | Ensure that at least 3 test drivers react appropriately to the selected Max_Torque_Amplitude | Ensure that when the torque amplitude crosses Max_Torque_Amplitude, the torque is set to zero within the fault tolerant time interval |
| Functional Safety Requirement 01-02 | Ensure that at least 3 test drivers react appropriately to the selected Max_Torque_Frequency | Ensure that when the torque frequency crosses Max_Torque_Frequency, the torque is set to zero within the fault tolerant time interval |

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

Lane Keeping Assistance (LKA) Requirements:

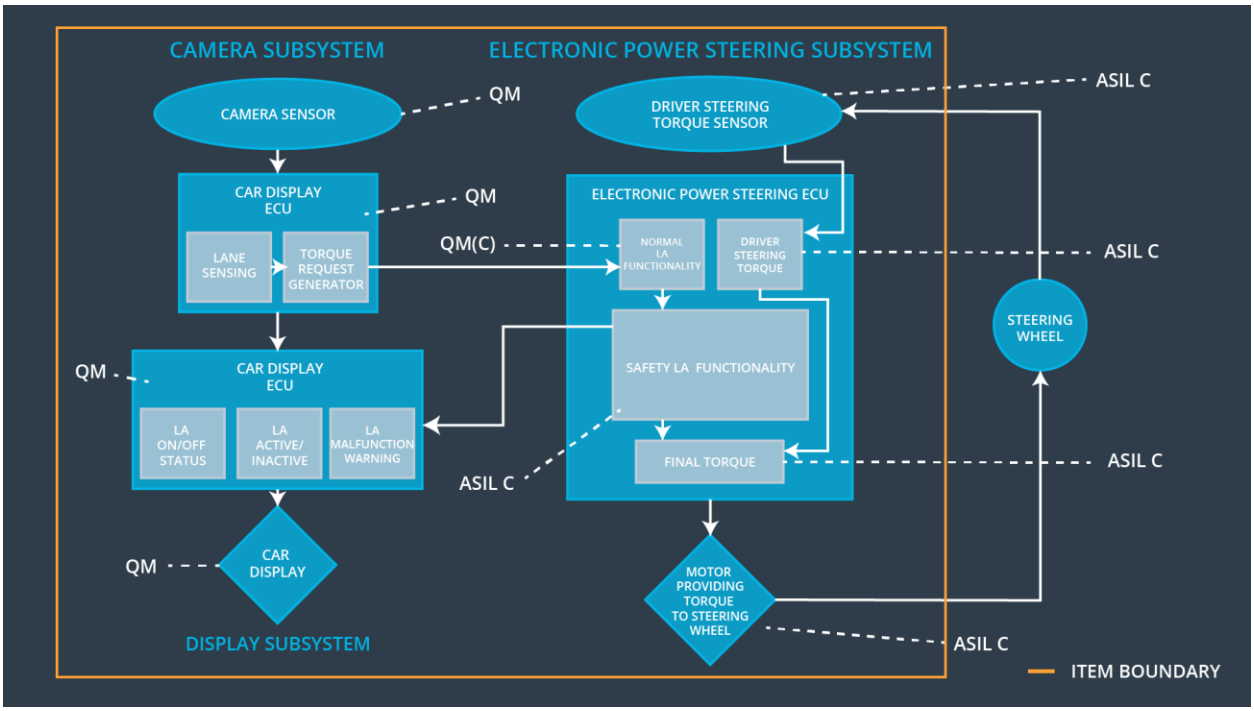
| ID | Functional Safety Requirement | ASIL | Fault Tolerant Time Interval | Safe State |
|---|---|---|---|---|
| Functional Safety Requirement 02-01 | The lane keeping item shall ensure that the lane keeping assistance function is torque is applied for only Max_Duration | B | 500 ms | The lane keeping item shall be disabled, output should be zero |

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 | Ensure that at least 3 test drivers react appropriately to the selected Max_Duration | Ensure that the lane keeping item is disabled after the lane keeping assistance function applies a torque for the Max_Duration + fault tolerant time interval |

## 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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude | **o** | | |
| Functional Safety Requirement 01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency | **o** | | |
| Functional Safety | The lane keeping item shall ensure that the lane keeping | **o** | | |

| | | | | |
|---|---|---|---|---|
| Requirement 02-01 | assistance function is torque is applied for only Max_Duration | | | |

## 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 functionality | Malfunction_01 | Yes | Warning light on the dashboard |
| WDC-02 | Turn off functionality | Malfunction_02 | Yes | Warning light on the dashboard |