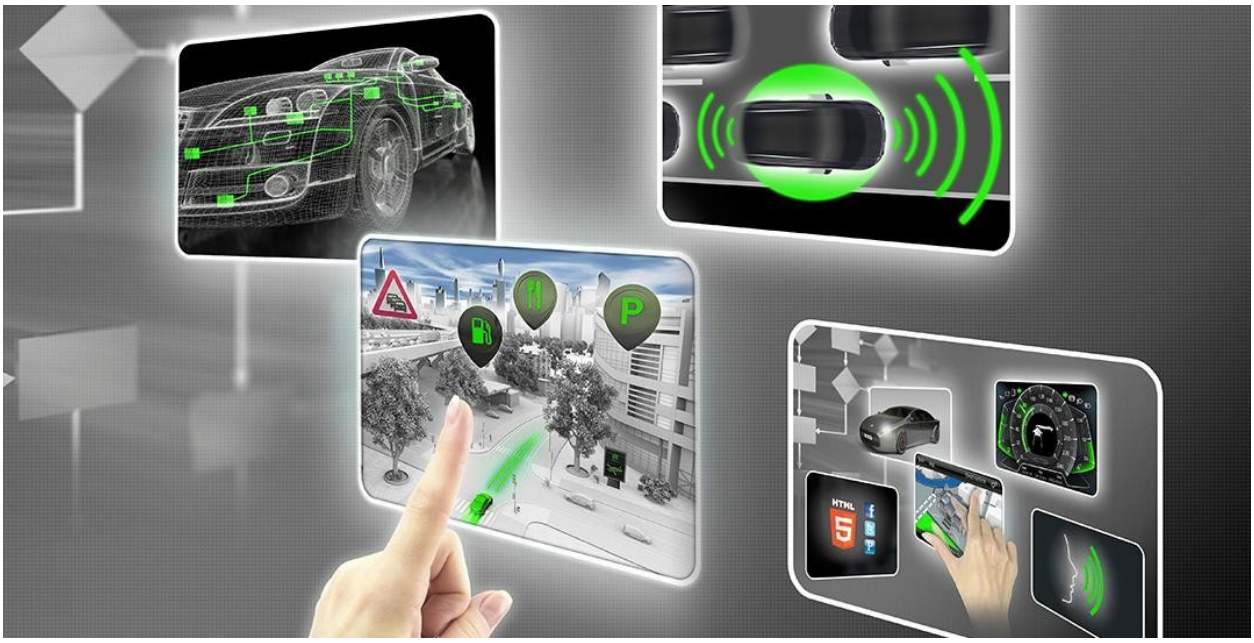
Elektrobit

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

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?]

1. Turning safety goal into functional safety requirements.
2. Allocating functional safety requirements to the item architecture.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

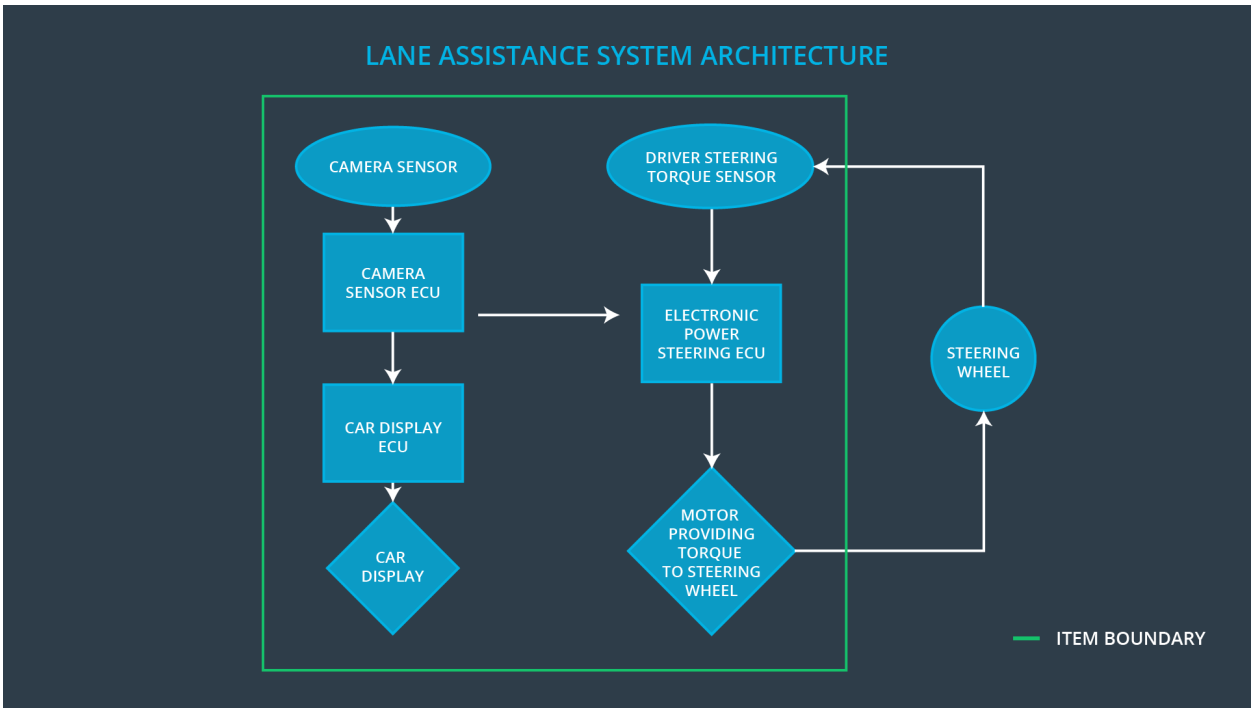
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

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 function shall be limited.
Safety_Goal_02	The lane keeping assistance function shall be time limited and addtional steering torque shall end after a given timer interval so that the driver cannot misuse the system for autonomous driving.

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	Senses that the vehicle is leaving the lane
Camera Sensor ECU	Detects the lane and provides the vibrational steering torque
Car Display	Shows a warning light to warn the driver
Car Display ECU	Controls a light to tell the driver that the function is activated
Driver Steering Torque Sensor	Detects how much the driver is already turning
Electronic Power Steering ECU	Provides a final torque to the motor based on the steering torque the driver has applied, and vibrational torque request from the camera subsystem
Motor	Applies the extra torque to the steering wheel

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 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 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 departure warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 ms	The amplitude and frequency of lane departure warning torque are set to zero.
Functional Safety Requirement 01-02	The lane departure warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 ms	The amplitude and frequency of lane departure warning torque is set to 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	If the chosen oscillating torque amplitude is below Max_Torque_Amplitude, the driver will not lose control and can feel the vibration.	when the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval.
Functional Safety Requirement 01-02	If the chosen oscillating torque amplitude is below Max_Torque_Frequency, the driver will not lose control and can feel the vibration.	when the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval.

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

Lane Keeping Assistance (LKA) Requirements:

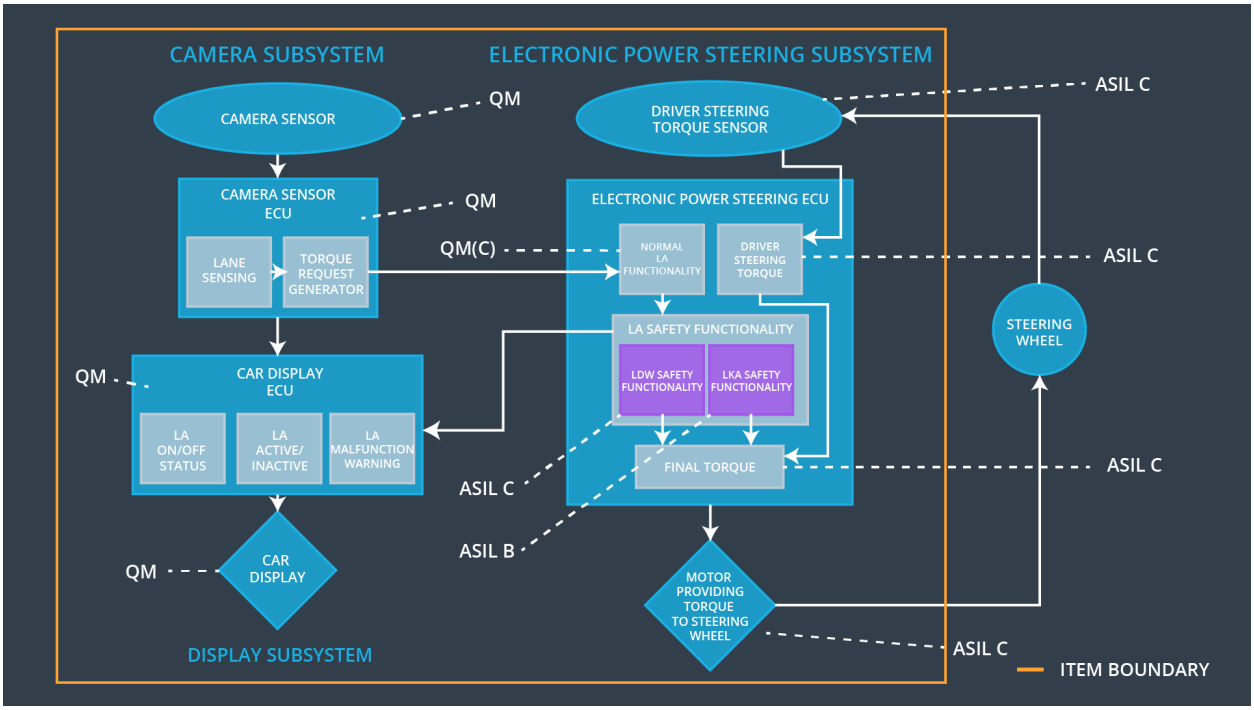
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The lane keeping assistance function can not be activated for more than max_duration.	B	500 ms	The lane keeping assistance torque is set to 0.

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	If the duration of the lane keeping assistance doesn't exceed the max_duration, then the driver will not take their hands off the wheel.	The system really does turn off if the lane keeping assistance exceeded max_duration.

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 departure item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	**x**		
Functional Safety Requirement 01-02	The lane departure item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	**x**		
Functional Safety Requirement 02-01	The lane keeping assistance function can not be activated for more than 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 the lane departure warning off	Malfunction_01, Malfunction_02	yes	Warning on car display
WDC-02	Turn off the lane keeping assistance off	Malfunction_03	yes	Warning on car display