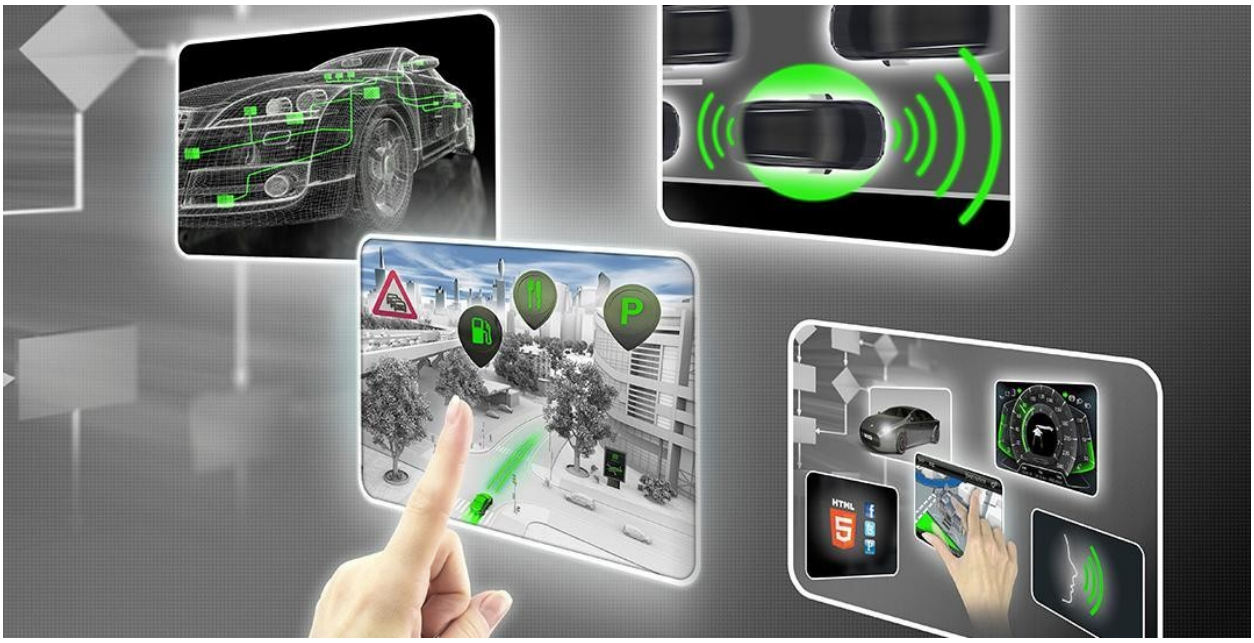
Elektrobit

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
25-08-2017	1.0	Ahmed Ghazal	Initial Draft

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 functional safety concept defines the functional requirements that will ensure that the safety goals are achieved.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

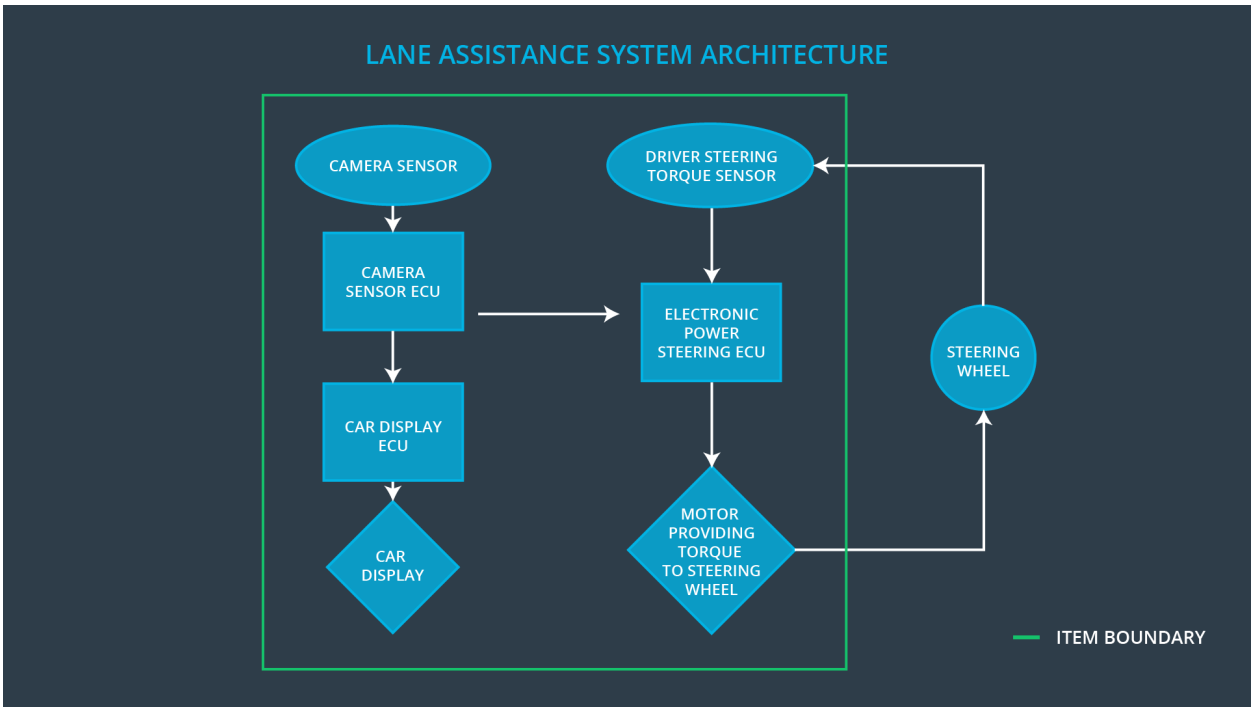
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

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 the additional steering torque shall end after a given time.
Safety_Goal_03	The Lane Keeping Assistance function shall provide an additional torque with a small threshold.
Safety_Goal_04	The Lane Departure Warning function shall provide an even oscillating torque to avoid car drifting.

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	Streams video of the road.
Camera Sensor ECU	Performs image processing on the captured images to detect the car’s position with respect to the lane.
Car Display	Displays a warning sign when the car is moving away from the lane.
Car Display ECU	Takes the car’s position as input from the Camera Sensor ECU and decides whether to display the warning sign or not.
Driver Steering Torque Sensor	Reads the current torque applied by the steering wheel.
Electronic Power Steering ECU	Takes the car’s position and the current torque as inputs, and decides whether an extra torque should be applied or not.
Motor	Provides the 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 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	A	Fault	Safe State

		SIL	Tolerant Time Interval	
Functional Safety Requirement 01-01	The Lane Departure Warning item shall ensure that the oscillating torque amplitude is below Max_Torque_Amplitude.	C	50ms	The Lane Departure Warning function is turned off.
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the oscillating torque frequency is below Max_Torque_Frequency.	C	50ms	The Lane Departure Warning function is turned off.

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 different torque amplitudes and observe how drivers react to each value to prove that the chosen value is the most convenient one.	Using a debug software that causes the torque amplitude to go over Max_Torque_Amplitude and verify that the system as a result sets the torque to zero within the fault tolerant time interval.
Functional Safety Requirement 01-02	Test different torque frequencies and observe how drivers react to each value to prove that the chosen value is the most convenient one.	Using a debug software that causes the torque frequency to go over Max_Torque_Frequency and verify that the system as a result sets the torque 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	The Lane Keeping Assistance function shall be time limited and the additional	B	500ms	The Lane Keeping

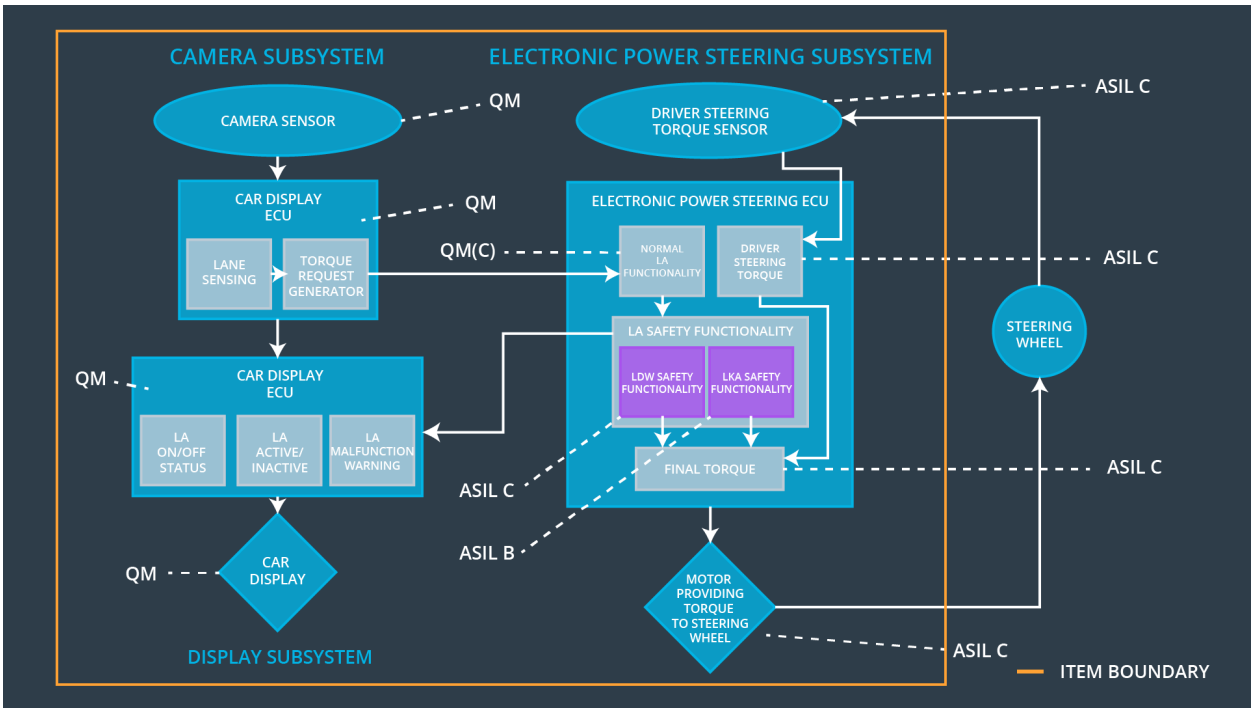
Requirement 02-01	steering torque shall end after a given timer interval.			Assistance function is turned off.

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	Validate that the max_duration chosen really did dissuade drivers from taking their hands off the wheel.	Verify that the system really does turn off if the lane keeping assistance every 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		X		
Functional Safety Requirement 01-02		X		
Functional Safety Requirement 02-01		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	Function is turned off.	Oscillating torque exceeds the maximum amplitude or frequency.	Yes	Warning sign on the car display indicating that Lane Departure Warning function is turned off.
WDC-02	Function is turned off.	Additional torque is applied for a time larger than the maximum limit.	Yes	Warning sign on the car display indicating that the Lane Keeping Assistance function is turned off.