



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
05/05/2019	0.1	Maanadoona	First 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]

[Document history](#)

[Table of Contents](#)

[Purpose of the Functional Safety Concept](#)

[Inputs to the Functional Safety Analysis](#)

[Safety goals from the Hazard Analysis and Risk Assessment](#)

[Preliminary Architecture](#)

[Description of architecture elements](#)

[Functional Safety Concept](#)

[Functional Safety Analysis](#)

[Functional Safety Requirements](#)

[Refinement of the System Architecture](#)

[Allocation of Functional Safety Requirements to Architecture Elements](#)

[Warning and Degradation Concept](#)

Purpose of the Functional Safety Concept

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

Ultimate goal of functional safety is avoiding accidents by reducing risk to acceptable levels

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.

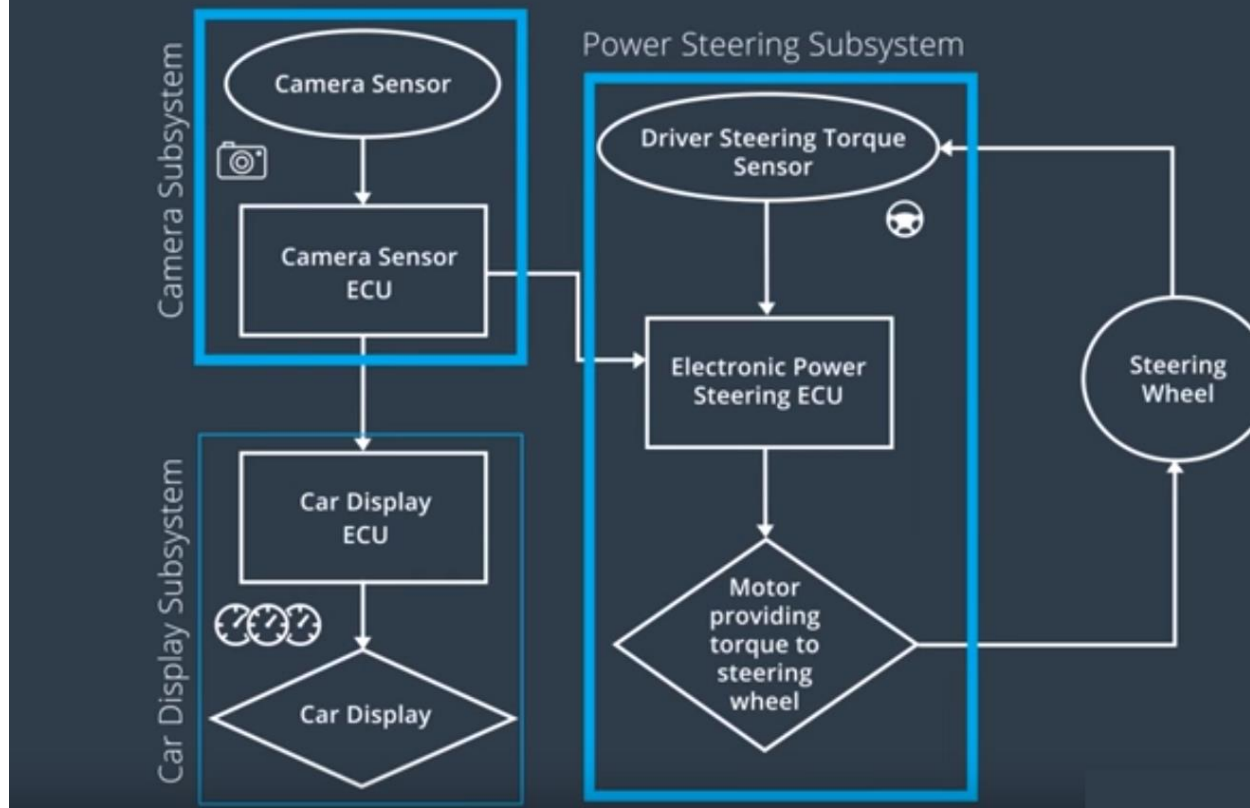
]

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 interval so that the driver cannot misuse the system for autonomous driving.
Safety_Goal_03	The LDW indication shall indicate the direction correctly
Safety_Goal_04	The lane keeping assistance function shall indicate the it's malfunction.

Preliminary Architecture

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

LANE ASSISTANCE SYSTEM ARCHITECTURE



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 reads in images from the road.
Camera Sensor ECU	The Camera Sensor ECU identifies when the vehicle has accidentally departed its lane, and sends the appropriate messages to the Car Display ECU and the Electronic Power Steering ECU.
Car Display	Indicate the information of camera
Car Display ECU	Controller to show the Warning and status of Lane Departure Assistance and Lane Keeping Assistance.
Driver Steering Torque Sensor	Measure the torque of steering wheel
Electronic Power Steering ECU	Device to control and sense the motor actuator

Motor	Actuator for applying 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.

Malfunction_04	Lane Departure Warning (LDW) function shall receive the signal from camera sensor to decide the direction.	WRONG	The Lane Departure Warning function is deactivated when the camera sensor is not working
Malfunction_05	Lane Keeping Assistance (LKA) function shall receive the signal from camera sensor to keep the lane.	WRONG	The Keeping Assistance function is deactivated when the camera sensor is not working

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	Vibration torque amplitude below Max_Torque_Amplitude.
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	Vibration frequency is below Max_Torque_Frequency.
Functional Safety Requirement 01-03	The Lane Departure Warning function is deactivated when the camera sensor is not working	QM	50 ms	Function is deactivated.

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

ID	Validation Acceptance	Verification Acceptance
----	-----------------------	-------------------------

	Criteria and Method	Criteria and Method
Functional Safety Requirement 01-01	Validate Max_Torque_Amplitude chosen is high enough to be detected by a driver while low enough not to cause loss of steering	Verify the system does turn off if the Lane Departure Warning exceeded Max_Torque_Amplitude.
Functional Safety Requirement 01-02	Validate Max_Torque_Frequency chosen is adequate to be detected by the driver and not cause the loss of steering.	Verify the system does turn off if the Lane Departure Warning exceeded Max_Torque_Frequency.
Functional Safety Requirement 01-03	Validate Lane Departure Warning is off when the camera sensor give the wrong signal.	Verify the Lane Departure Warning is deactivated when the camera sensor is wrong.

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

Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	A S I L	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only Max_Duration.	B	500 ms	Lane Keeping Assistance torque is zero.
Functional Safety Requirement 02-02	The Keeping Assistance function is deactivated when the camera sesor is not woking	C	50 ms	Function is deactivated.

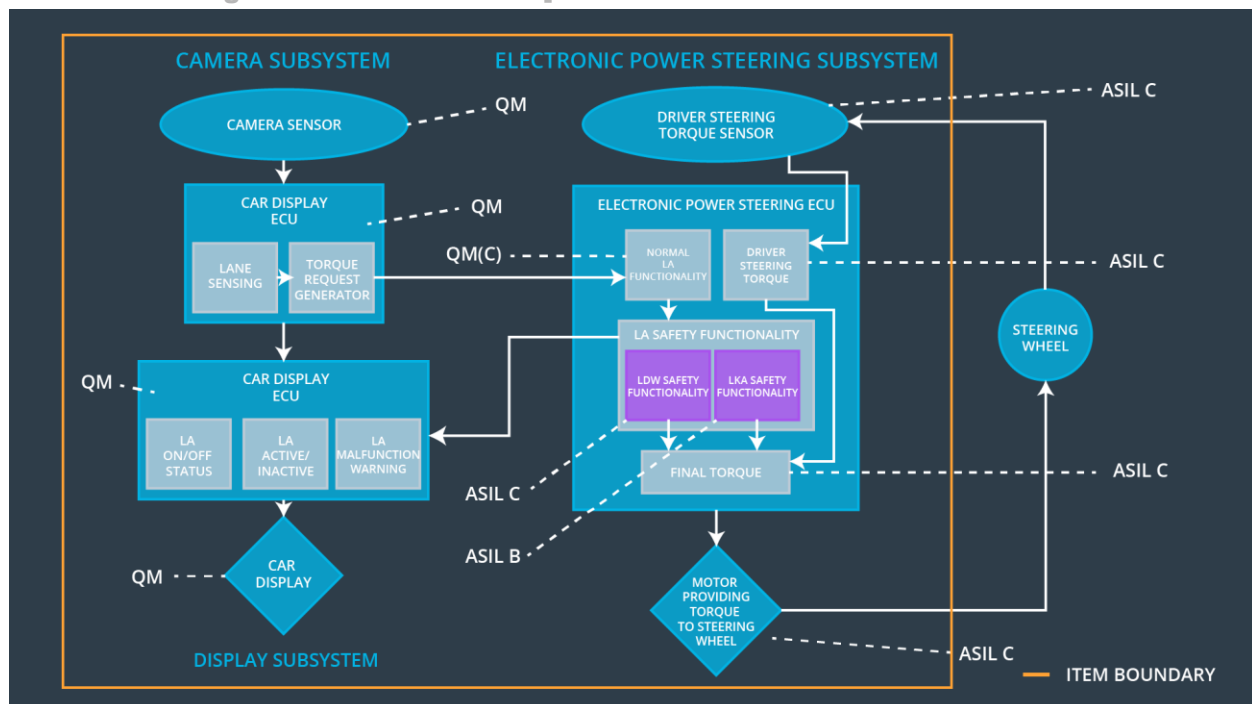
Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety	Validate the Max_Duration chosen not allow the driver to use the car as self-	Verify the system does deactivate if the Lane Keeping Assistance torque

Requirement 02-01	driving car.	application exceeded Max_Duration.
Functional Safety Requirement 02-02	Validate the Lane Keeping assistance shall be deactivated when the camera sensor is broken.	Verify the Lane Keeping Assistance is deactivated if the camera sensor is not working.

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	Camera ECU	Car Display ECU

		ECU		
Functional Safety Requirement 01-01	The Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	X		
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	X		
Functional Safety Requirement 01-03	The Lane Departure Warning function is deactivated when the camera sesor is not woking		X	
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only Max_Duration.	X		
Functional Safety Requirement 02-02	The Keeping Assistance function is deactivated when the camera sesor is not woking		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 Lane Departure Warning functionality	Malfunction_01, Malfunction_02, Malfunction_04	Yes	Lane Departure Warning Malfunction Warning on Car Display

WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03, Malfunction_05	Yes	Lane Keeping Assistance Malfunction Warning on Car Display
--------	------------------------------------------------	--------------------------------	-----	------------------------------------------------------------