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
16-05-2018	1.0	Disha Patel	Initial Submission
19-05-2018	2.0	Disha Patel	Update after first review

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 functional safety is to avoid accidents by reducing risk to acceptable levels.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

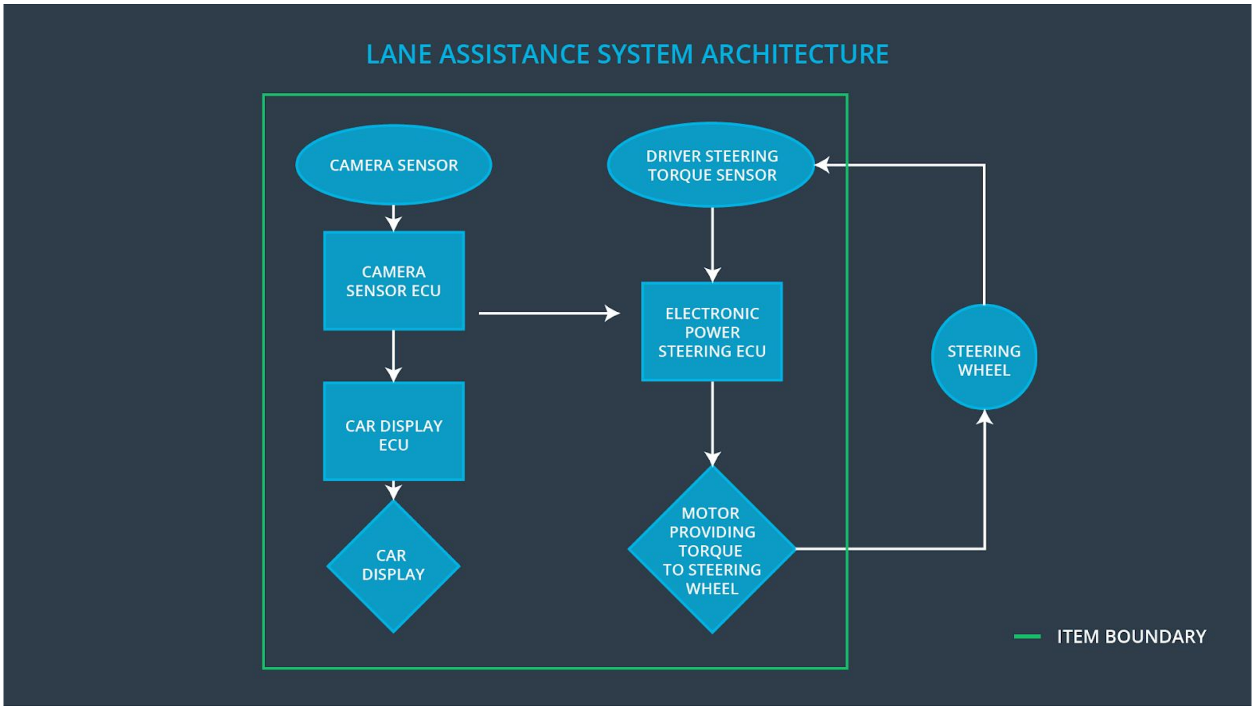
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

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

ID	Safety Goal
Safety_Goal_01	For the lane departure warning function, the oscillating steering torque from the function shall be limited. S3 x E3 x C3 = ASIL C
Safety_Goal_02	The lane keeping assistance function should be time limited and the additional steering torque should end after a mentioned time interval so the system for autonomous driving is not misused by the driver. = ASIL B

Preliminary Architecture

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


LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
CAMERA SENSOR ECU
CAR DISPLAY ECU
CAR DISPLAY
DRIVER STEERING TORQUE SENSOR
ELECTRONIC POWER STEERING ECU
MOTOR PROVIDING TORQUE TO STEERING WHEEL
STEERING WHEEL
ITEM BOUNDARY

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	To provide the images captured from camera to the camera Sensor ECU.
Camera Sensor ECU	Images will be analyzed and will calculate the car position and detect the lane lines.
Car Display	It will display warning to the driver.
Car Display ECU	It will show the lane departure and lane keeping assistance warning status, by controlling the car display component.
Driver Steering Torque Sensor	It will be measuring the steering torque which will be applied by the driver to the steering wheel.
Electronic Power Steering ECU	It will process the inputs from Driver steering torque sensor, Camera Sensor ECU and request

	the required torque which will be applied by the motor.
Motor	It will apply the torque received from Electronic Power Steering ECU and apply it 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 oscillating amplitude is too high.
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	The oscillating frequency is too high.

Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	NO	the lane departure oscillating torque amplitude is below Max_Torque_Amplitude

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 oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Set vibration torque amplitude to zero
Functional Safety Requirement 01-02	the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	Set vibration torque frequency to zero

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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional	Validating the Max_Torque_Amplitude and check if	To verify that the system goes turn off when the

Safety Requirement 01-01	it is low which will not cause the steering loss.	Max_Torque_Amplitude is exceeded.
Functional Safety Requirement 01-02	Validating the Max_Torque_Frequency and check if it is low which will not cause the steering loss.	To verify that the system goes turn off when the Max_Torque_Frequency is exceeded.

[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	Lane keeping assistance function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver cannot misuse the system for autonomous driving	B	500 ms	Set lane keeping assistance torque to be zero

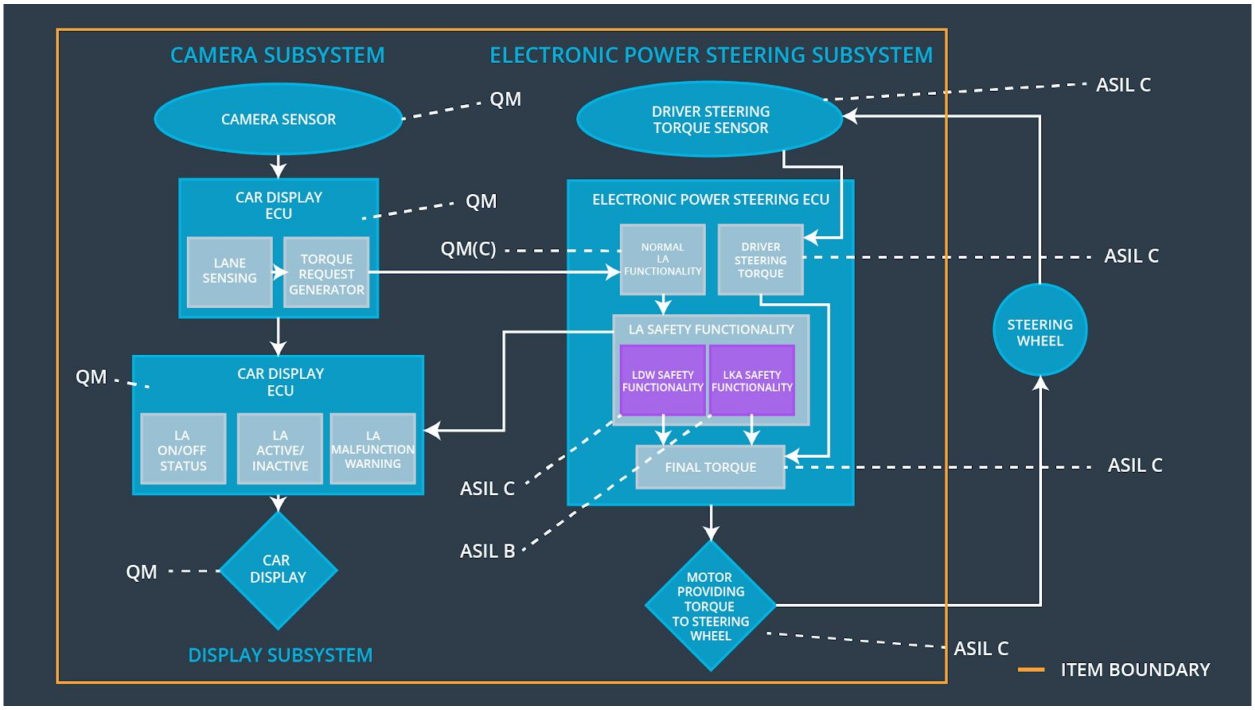
Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement	The max_duration chosen really did dissuade drivers from taking their hands off the wheel	The system really does turn off if the lane keeping assistance every exceeded max_duration.

02-01		

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	The electronic power steering	x		

Safety Requirement 01-01	ECU should be ensuring that the lane departure oscillating torque frequency is below Max_Torque_Frequency			
Functional Safety Requirement 01-02	The electronic power steering ECU should be ensuring that the lane departure oscillating torque Amplitude is below Max_Torque_Amplitude	**x**		
Functional Safety Requirement 02-01	The electronic power steering ECU should be ensuring that the lane keeping torque is applied for less than the Max_Duration.	**x**		

Warning and Degradation Concept

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

WDC-01 is for Lane Departure Warning function
WDC-02 is for Lane Keeping assistance function

ID	**Degradation Mode**	**Trigger for Degradation Mode**	**Safe State invoked?**	**Driver Warning**
WDC-01	Turn off the functionality	Malfunction_01 Malfunction_02	Yes	a warning light on the dashboard
WDC-02	Turn off the functionality	Malfunction_03	Yes	a warning light on the dashboard