Functional Safety Concept Lane Assistance

Document history

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
9/1/2017	1.0	Xu fuqiang	submit version

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

The purpose of a functional safety concept is to identify new requirements from safety goals and then allocate those requirements to different parts of the item architecture from a higher level.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

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.

Preliminary Architecture
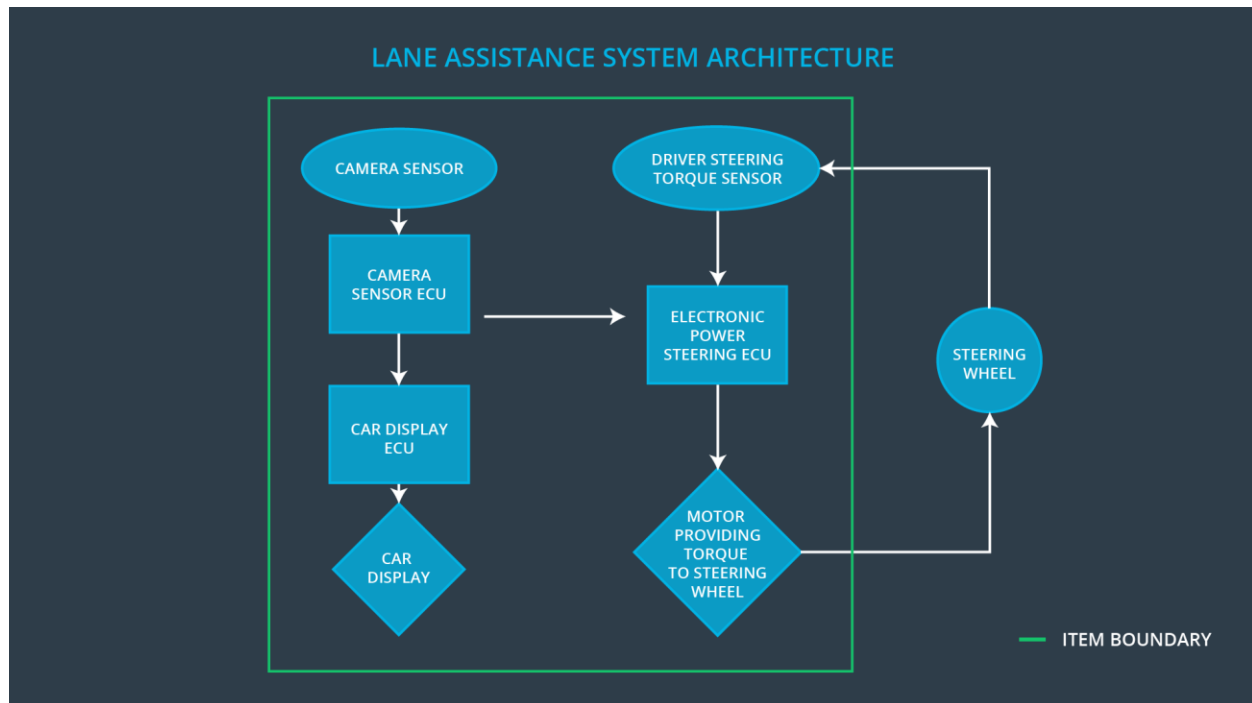
Description of architecture elements

[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 it lane, and sends the appropriate messages to the Car Display ECU and the Electronic Power Steering ECU.
Car Display	The Car Display turns on warning light to alert driver.
Car Display ECU	The Car Display ECU receives signals from camera sensor ECU and control Car Display to alert driver.
Driver Steering Torque Sensor	The Driver Steering Torque Sensor measures the torque provided by driver.
Electronic Power Steering ECU	The Electronic Power Steering ECU determines final appropriate torques based on lane assistance system torque request.
Motor	The Motor applies appropriated torques required to get the car back towards center to steering wheels.

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

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	50ms	LDW torque output is set to 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	50ms	LDW torque output 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	Need to test how drivers react to different torque amplitudes to prove that we chose an appropriate value	Need to verify that the safety requirement is met; 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	Need to test how drivers react to different torque frequencies to prove that we chose an appropriate value	Need to verify that the safety requirement is met; when the torque frequencies crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval.

Lane Keeping Assistance (LKA) Requirements:

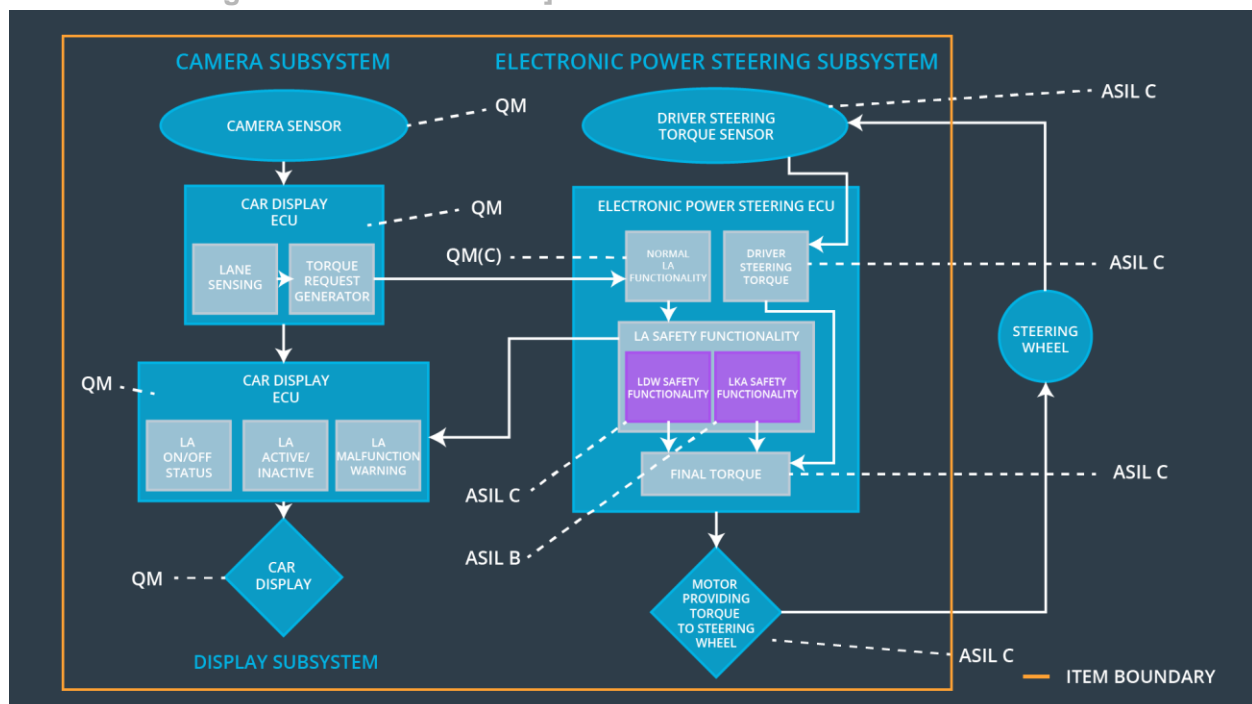| ID	Functional Safety Requirement	A	Fault	Safe State

		S I L	Tolerant Time Interval	
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500ms	LKA torque output is set to 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	Need to test and validate that the max_duration chosen really did dissuade drivers from taking their hands off the wheel	Need to 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	The electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	**X**		
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	**X**		
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only 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 functionality	Torque amplitude or	Yes	Yes

		frequencies beyond allowed maximum		
WDC-02	turn off the functionality	the lane keeping assistance goes beyond the time limit we set	Yes	Yes