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
9/19/2017	1.0	Guru Shetti	Initial version
9/29/2017	1.1	Guru Shetti	Incorporated feedback from 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]

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?]

The purpose of functional safety concept is to identify which subsystems and elements can be used to meet safety goals, and allocates functional safety requirements to the relevant parts in the system architecture. Allocation could involve expanding the system architecture with new element blocks.

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.
]

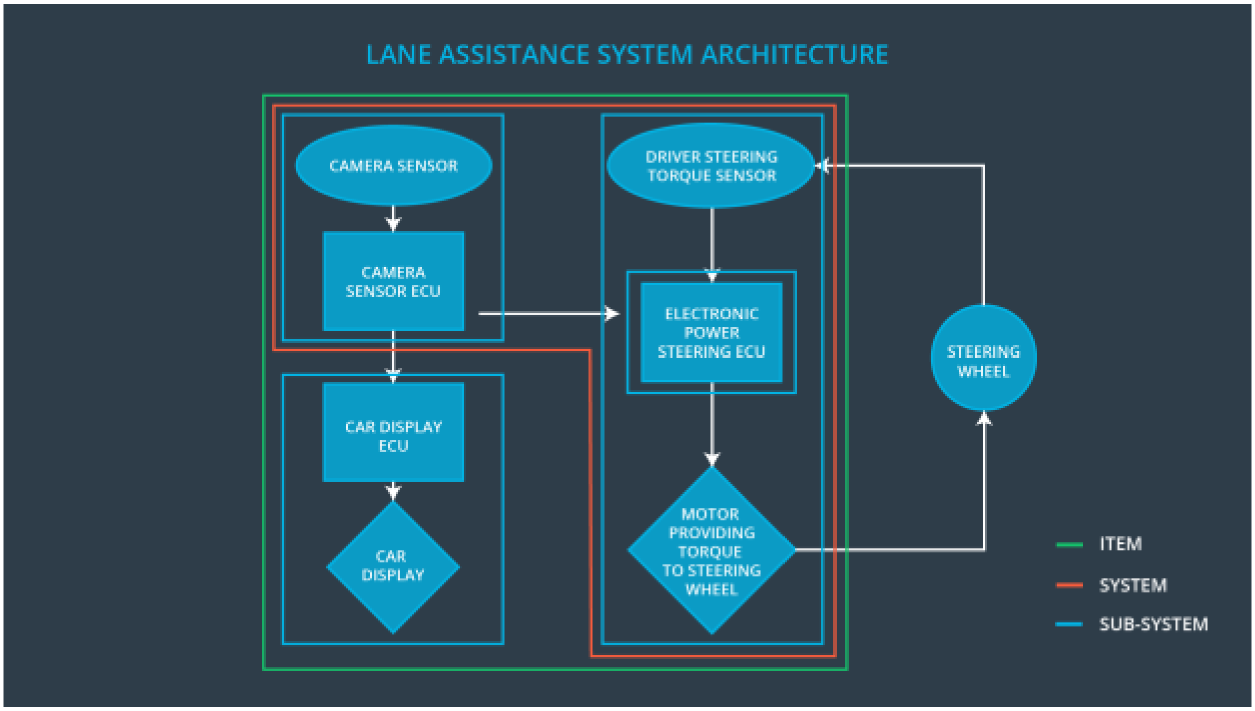
ID	Safety Goal
Safety_Goal_01	The oscillating steering torque from the lane departure warning function shall be limited
Safety_Goal_02	When lane structure is not understood driver should be warned with light in driver panel and haptic feedback at steering
Safety_Goal_03	LKW should deactivate during unpredictable conditions
Safety_Goal_04	The LKA system should check if the Electronic Power Steering ECU is functioning and give warning to driver if it stops working.

Preliminary Architecture

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

The top-level lane architecture is given below in green. ECU stands for Electronic Control Unit. An ECU is a small computer that contains the hardware and software for a specific vehicle

functionality. The camera ECU, for example, might have the hardware and software required for deep learning or for computer vision techniques like the Hough transform.
To summarize the functionality, the camera system detects lane departures and tells the steering wheel how hard to turn. The driver receives a warning on the vehicle display and also receives a warning via a steering wheel vibrating. Simultaneously, the wheel adds extra steering torque to help the driver move back towards the center of the lane.


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
SYSTEM
SUB-SYSTEM

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	Capture and stream images to Camera Sensor ECU for processing
Camera Sensor ECU	Processes image stream from camera sensor to detect lane lines on the road and determine if the vehicle is moving out of the lane unintentionally
Car Display	LCD or other visual interface used to display the warning messages and setting changes.

Car Display ECU	Processes input from camera subsystem and display the messages on the Car Display
Driver Steering Torque Sensor	Responsible for measuring the torque applied by the driver.
Electronic Power Steering ECU	Vibrates the steering wheel when vehicle is drifting away from the current lane unintentionally. Add appropriate amount of torque based on feedback from torque sensor to keep vehicle in current lane.
Motor	Actuator used to apply requested torque to 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	MORE	LKW should deactivate during unpredictable conditions

	an oscillating steering torque to provide the driver a haptic feedback		
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	**NO**

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 electronic power steering subsystem shall ensure that the oscillating torque amplitude is less than Max_Torque_Amplitude	C	50ms	**Turning off of the lane departure warning function**
Functional Safety Requirement 01-02	The electronic power steering subsystem shall ensure that the oscillating torque frequency is less than Max_Torque_Frequency	C	50ms	**Turning off of the lane departure warning function**

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 how drivers react to different torque amplitudes to prove that we chose an appropriate value	Verify that when the torque amplitude crosses the limit, the lane assistance output is set to zero within the fault tolerant time interval
Functional Safety Requirement 01-02	Test how drivers react to different torque frequencies to prove that we chose an appropriate value	Verify that when the torque frequency crosses the limit, the lane assistance output is set 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:

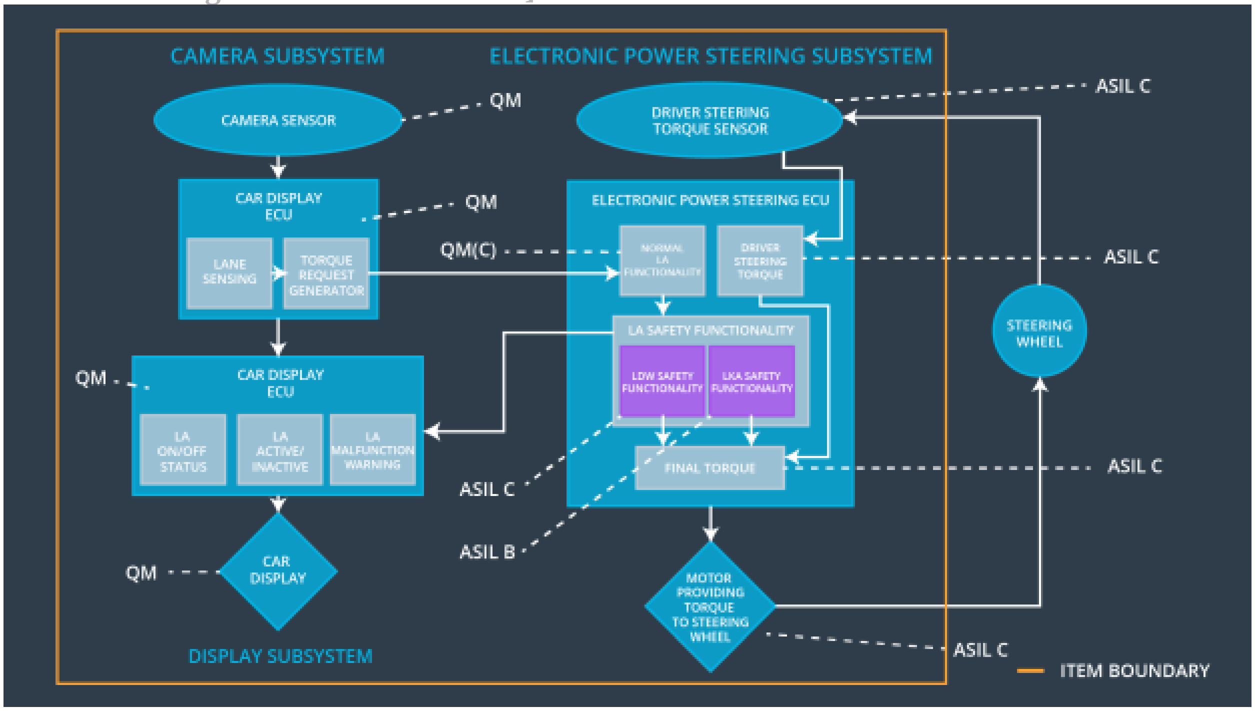
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500ms	**Turning off of the lane keeping assistance function**

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.]



The camera sensor ECU has two software blocks:

1. **Lane Sensing** – detect the lane and check if the vehicle is moving away from the ego lane.
2. **Torque Request Generator** – send a torque request to the electronic power steering subsystem

The car display subsystem has three software blocks:

1. **LA ON/OFF Status** – control a light that tells the driver if the lane keeping system on or off.
2. **LA Active/Inactive** – control a light telling the driver that if the lane departure warning is activated.
3. **LA Malfunction Warning** – display warning message if LA system is malfunctioning.

The electronic power steering subsystem has three software blocks:

1. **Normal Lane Assistance Functionality** – receive the vibrational torque request form camera subsystem.
2. **Driver Steering Torque** – sense how much the driver is turning the steering wheel.
3. **Final Torque** – add torque requests together to output a final torque to the motor that move the steering wheel.

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 oscillating torque amplitude is below Max_Torque_Amplitude	**YES**		
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the oscillating torque amplitude is below Max_Torque_Amplitude	**YES**		
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the oscillating torque amplitude is below Max_Torque_Amplitude	**YES**		

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	OFF	Oscillating torque frequency is higher than Max_Torque_Frequency or torque is higher than Max_Torque_Amplitude	Yes	Car Display
WDC-02	OFF	Lane keeping assistance torque is applied for more than Max_Duration	Yes	Car Display