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
10/Sep/2017	0.1	Andrew Wilkie	Updating while following T3.M2.E2.L17 videos

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 (aka document) is to provide a high level overview of the system.

Using the previously completed hazard analysis and risk assessment we will describe what the system is required to do in order to remain safe.

The document will also describe where the new safety changes will be made to the system.

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.
Lane Departure Warning : Reduce maximum steering oscillating torque to prevent occurrence of driver being unable to maintain grip on the steering wheel.

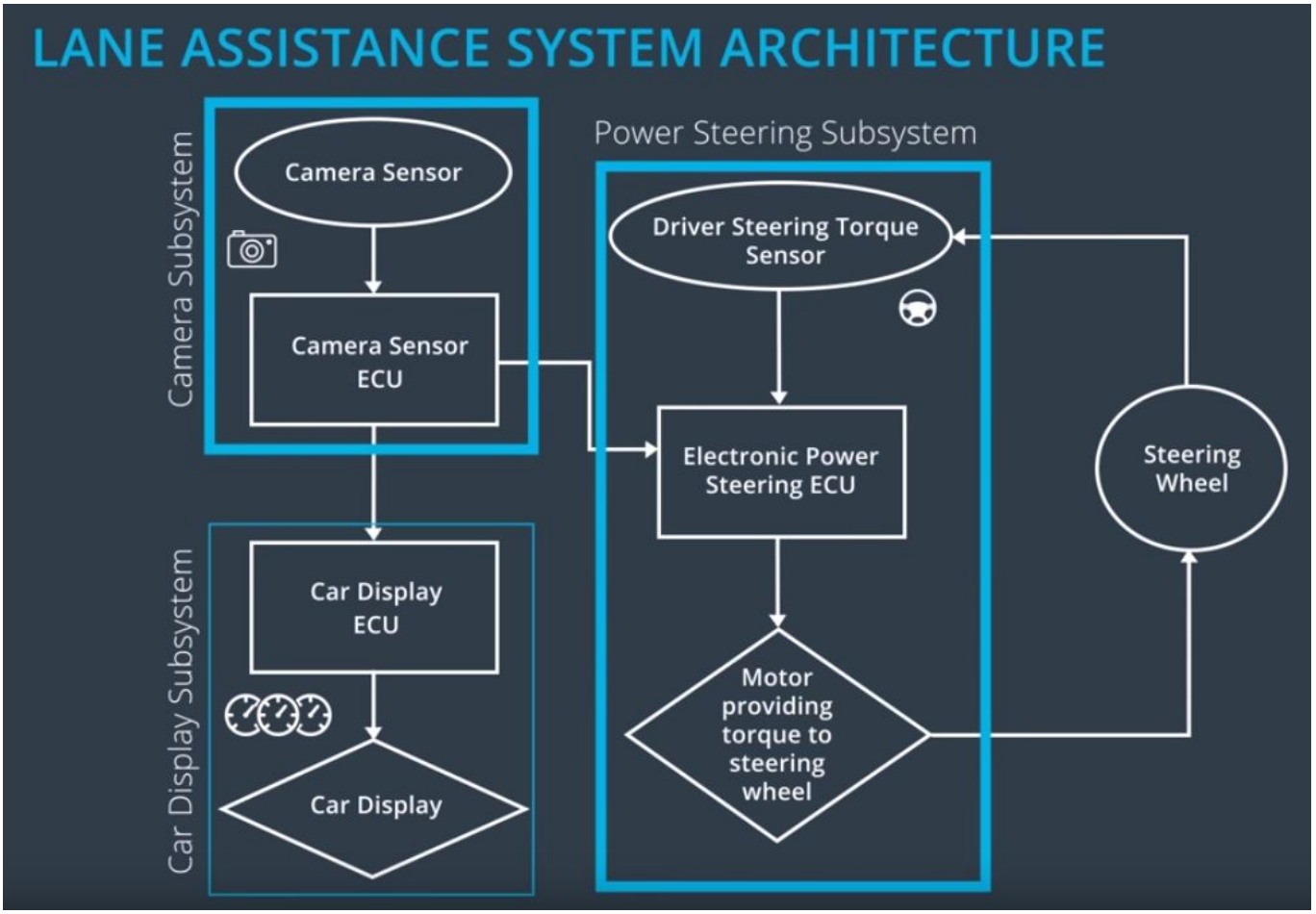
Lane Keeping Assistance : Set time limit on activation to prevent occurrence of driver intentionally removes hands from the steering wheel.

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

Preliminary Architecture

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

Diagram 1 : Lane Assistance Item 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?]

concept

Element	Description
Camera Sensor	Captures images within its field of view.
Camera Sensor ECU	Takes image input from the Camera Sensor to perform road lane detection and pass this information to both the Car Display ECU and the

	Electronic Power Steering ECU.
Car Display	Takes data input from Car Display ECU to display status and warning information to the driver.
Car Display ECU	Takes data input from Camera Sensor ECU and outputs data to the Car Display.
Driver Steering Torque Sensor	Takes data input from the Steering Wheel and outputs torque level information to the Electronic Power Steering ECU.
Electronic Power Steering ECU	Takes lane detection information input from Camera Sensor ECU and torque information from Driver Steering Torque Sensor and outputs instructions to the Motor.
Motor	Motor is an actuator that applies 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	ASIL	Fault Tolerant Time Interval	Safe State

Functional Safety Requirement 01-01	The electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	B	50 ms	Turn off by setting torque request to 0.
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	B	50 ms	Turn off by setting torque request to 0.

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

ID	V**alidation Acceptance Criteria and Method**	**Verification Acceptance Criteria and Method**
Functional Safety Requirement 01-01	Validate that the amplitude of the steering oscillation torque is not too high for the driver to handle or too low that the driver cannot feel the vibration.	Verify that steering oscillation torque amplitude is below Max_Torque_Amplitude.
Functional Safety Requirement 01-02	Validate that the frequency of the steering oscillation torque is not too high for the driver to handle or too low that the driver cannot feel the vibration.	Verify that steering oscillation torque amplitude is below Max_Torque_Frequency.

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

Lane Keeping Assistance (LKA) Requirements:

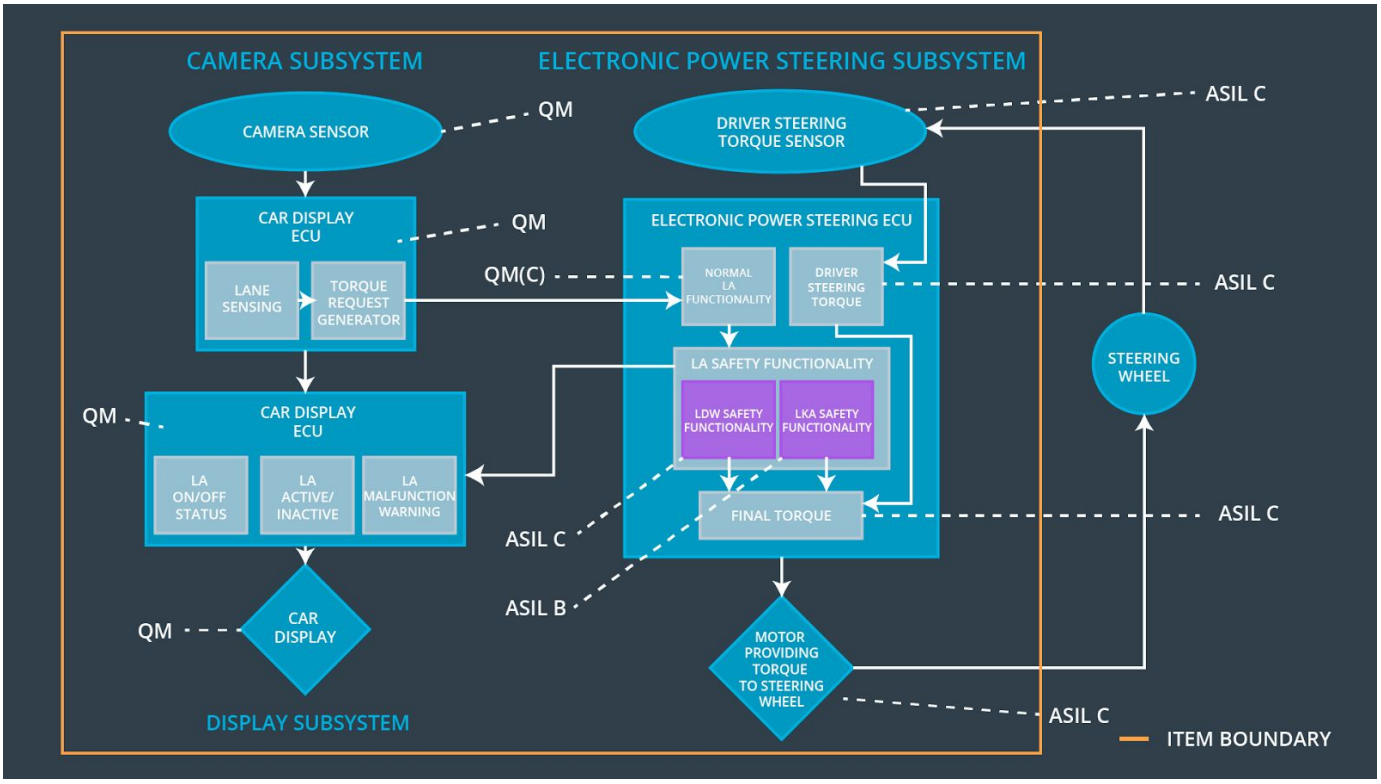
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	C	500 ms	Turn off function.

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 lane keeping assistance is applied for long enough to help the driver return safely to the lane centre but not active too long that the driver is tempted to incorrectly use it as an autonomous driving system.	Verify that the lane keeping assistance torque applied time length is below 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	Ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	X		

Functional Safety Requirement 01-02	Ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	X		
Functional Safety Requirement 02-01	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-01-01	Turn off function.	Steering oscillation torque amplitude is above Max_Torque_Amplitude.	Yes.	LDW Active / Inactive display indicates Inactive. LA Malfunction Warning display light is On.
WDC-01-02	Turn off function.	Steering oscillation torque amplitude is above Max_Torque_Frequency.	Yes.	LDW Active / Inactive display indicates Inactive.

				LA Malfunction Warning display light is On.
WDC-02-01	Turn off function.	Lane keeping assistance torque applied time length is above Max_Duration.	Yes.	LKA On / Off Status display indicates Off. LA Malfunction Warning display light is On.