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
Apr. 30, 19	1.0	Norihito Tohge	First attempt

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?]

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

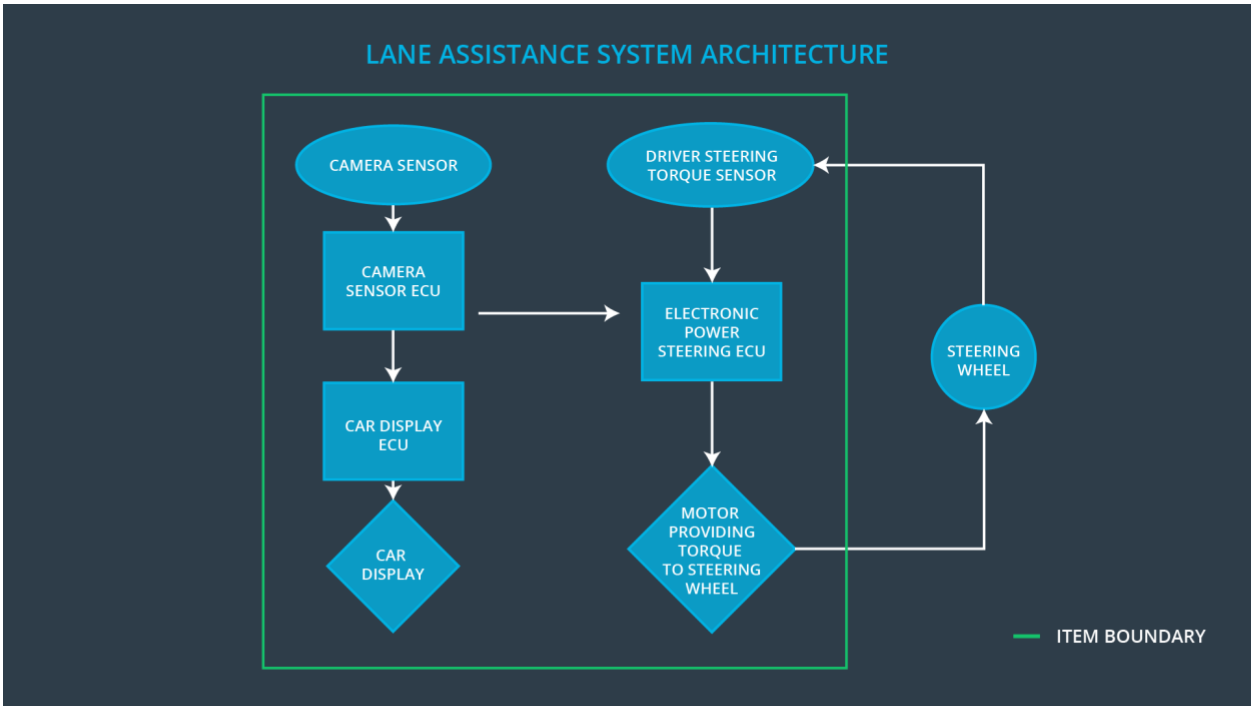
**[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.**

**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 torque to the steering wheel from the LKA function shall be limited.
Safety_Goal_02	The LKA 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

[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	Camera Sensor captures environment images in front of the vehicle and outputs them to Camera Sensor ECU.
Camera Sensor ECU	Camera Sensor ECU processes images from Camera Sensor and detect lanes in them. Based on the lane detection results, it also checks whether the car is not departing the lane for LDW function and the deviation from the center of the lane for LKA function. Then it outputs each results to Car Display ECU and Electronic Power Steering ECU.
Car Display	Car Display shows the status of LKA if activated and the warning of LDW if required.
Car Display ECU	Car Display ECU processes the input from Camera Sensor ECU and determines whether the status of LKA and/or the warning of LDW should be displayed on Car Display.
Driver Steering Torque Sensor	Driver Steering Torque Sensor senses the amount of

	torque applied to the steering wheel by the driver.
Electronic Power Steering ECU	Electronic Power Steering ECU calculates the torque to vibrate the steering wheel if LDW alert is requested and to move the steering wheel to keep the vehicle in the center of the lane based on the deviation of the vehicle if LKA is activated.
Motor	Motor applies torque to the steering wheel based on the result of Electronic Power Steering ECU torque calcuration.

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	MORE	The lane departure warning function applies an oscillating torque with very high torque frequency

	feedback		(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 Lane Assistance item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 ms	The system is turned off.
Functional Safety Requirement 01-02	The Lane Assistance item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 ms	The system is turned off.

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	Testing how drivers react to different torque amplitudes to choose an appropriate value.	Testing the software by inserting a fault and check if the system works as expected.
Functional	Testing how drivers react to different	Testing the software by inserting a

Safety Requirement 01-02	torque frequencies to choose an appropriate value.	fault and check if the system works as expected.

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

Lane Keeping Assistance (LKA) Requirements:

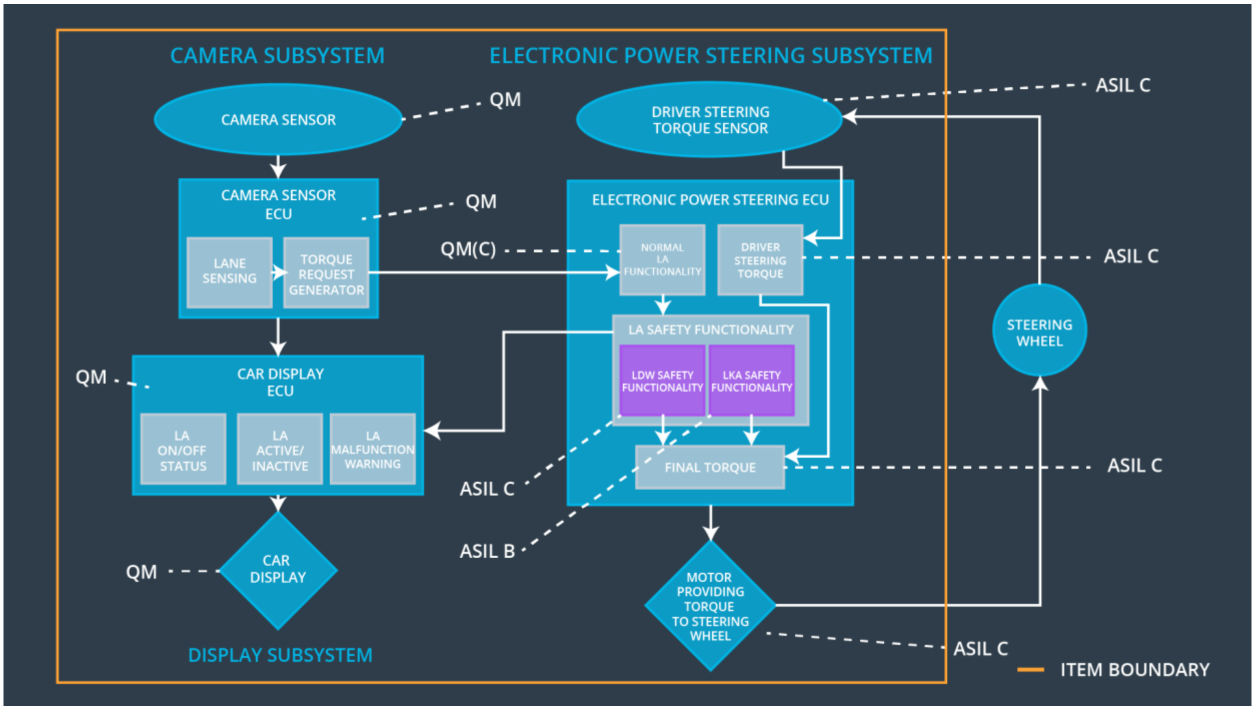
ID	**Functional Safety Requirement**	**ASIL**	**Fault Tolerant Time Interval**	**Safe State**
Functional Safety Requirement 02-01	The Electronic Power Steering ECU shall ensure that the Lane Keeping Assistance torque is applied for only Max_Duration.	B	500 ms	The system is turned off.

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	Testing various Max_Duration values to see how long drivers start to misuse the system.	Check if the system really turns off LKA if no driver torque applied for more than 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 Lane Assistance item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	**X**		
Functional Safety Requirement 01-02	The Lane Assistance item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	**X**		
Functional Safety Requirement	The Electronic Power Steering ECU shall ensure that the Lane Keeping Assistance torque is	**X**		

02-01	applied for only Max_Duration.			

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	Turning off the system	The lane departure oscillating torque exceeds Max_Torque_Amplitude or the lane departure oscillating frequency exceeds Max_Torque_Frequency.	Yes	A warning message is shown on Car Display.
WDC-02	Turning off the system	The Lane Keeping Assistance torque is applied for more than Max_Duration.	Yes	A warning message is shown on Car Display.