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
10/1/2017	1.0	Sumit Chhabra	Functional Safety Concept

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 (FSC) looks at the general functionality of the item, i.e., Vehicle Lane Assistance, without going into the technical details. FSC derives the safety goal requirements from Hazard Analysis and Risk Assessment where functions and malfunctions are analyzed methodically. FSC allocates these safety goal requirements to the system architecture diagrams, that will ensure the item behaves in the safe manner. Function Safety concept is the last phase of the concept phase in the V process model.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

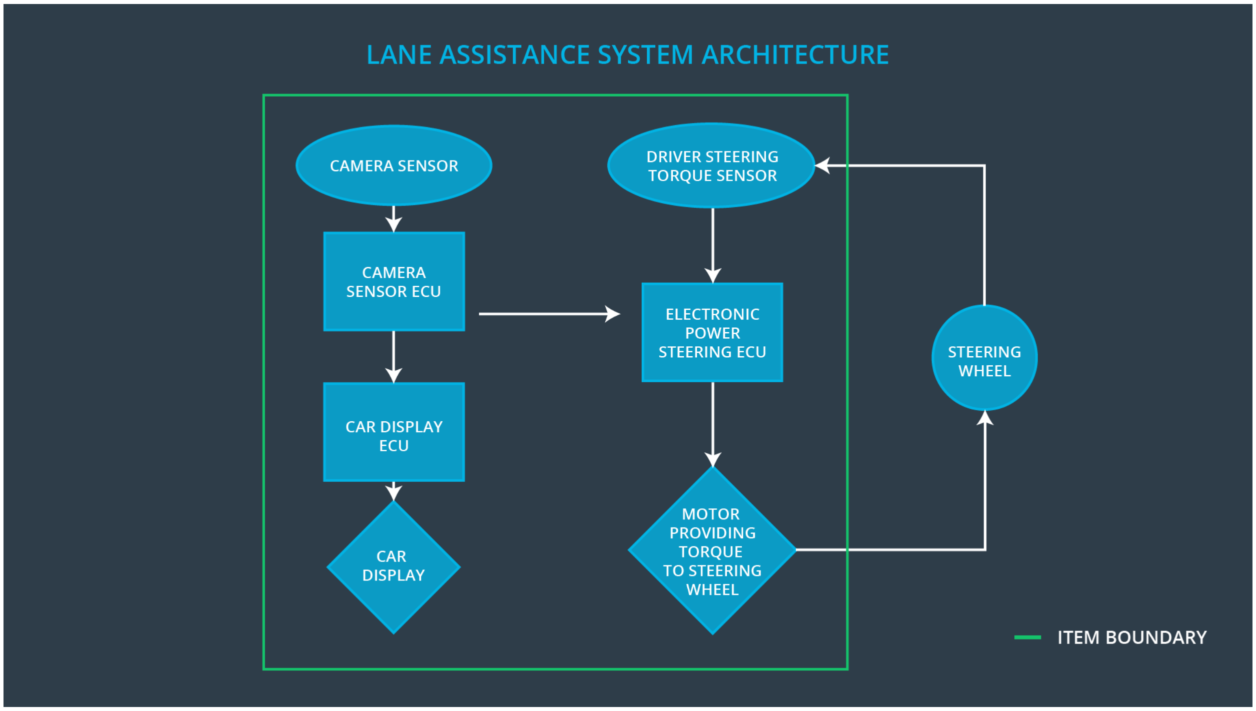
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

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	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

[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	Captures and sends the image frames of road to the camera sensor ECU.
Camera Sensor ECU	Using the information from camera sensor, it checks for the lane boundaries and send notification to the power steering ECU as well as car display system if care leaves the lane.
Car Display	Dashboard to show warning symbol with light on and off to the driver.
Car Display ECU	Takes the input from camera sensor ECU and controls the logic to display the warning in car display if LDW or LKW are detected.
Driver Steering Torque Sensor	Measures the torque applied by the driver.
Electronic Power Steering ECU	Takes input from camera ECU and driver steering torque sensor and calculates the necessary torque needed as well as time duration for LKA.

Motor	Takes the input from Electronic Power Steering ECU and provides the 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

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	LDW 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	LDW 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	LKA 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	Off
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	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	Define a reasonable limit for max torque amplitude for LDW. Test how drivers will react to different torque amplitudes.	If torque amplitude crosses the defined limit, the lane assistance output is set to zero within the 50ms fault tolerant time interval.
Functional Safety Requirement 01-02	Define a reasonable limit for max torque frequency for LDW. Test how drivers will react to different torque amplitudes.	If torque frequency crosses the defined limit, the lane assistance output is set to zero within the 50ms fault tolerant time interval.

Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement	The lane keeping item shall ensure that the lane keeping assistance torque is applied	B	500ms	Off

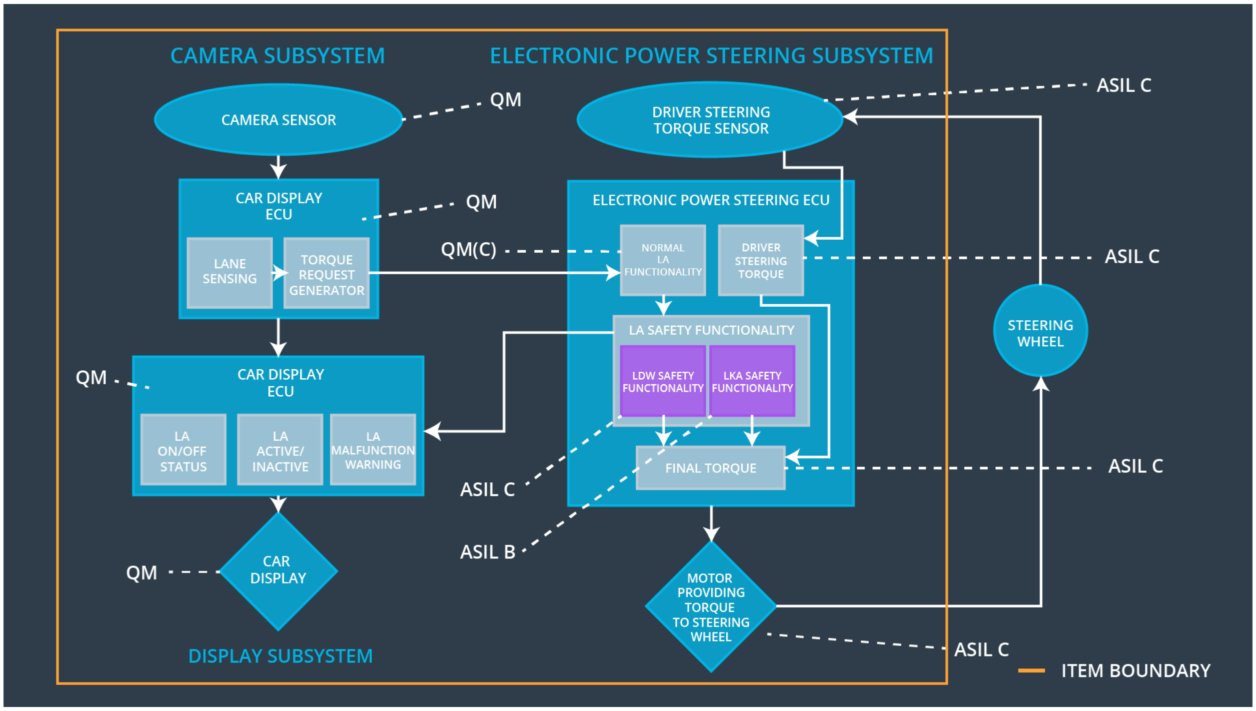
02-01	for only Max_Duration			

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	Define a reasonable limit for Max_Duration. Test and validate the chosen value resulted in dissuading the drivers from taking their hands off the wheel.	Verify the system turn off the LKA after Max_Duration is exceeded.

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	Electronic Power Steering ECU shall ensure torque amplitude shall not exceed Max_Torque_Amplitude.	**X**		
Functional Safety Requirement 01-02	Electronic Power Steering ECU shall ensure torque frequency shall not exceed Max_Torque_Frequency.	**X**		
Functional Safety Requirement 02-01	Electronic Power Steering ECU shall ensure LKA function will be time limited and steering torque ends after Max_Duration is exceeded,	**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	Off	If Torque amplitude exceeds Max_Torque_Amplitude or Torque	Yes	Warning light in car display

		frequency exceeds Max_Torque_Frequency		
WDC-02	Off	If LKA torque applied exceeds the Max_Duration time interval	Yes	Warning light in car display