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

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 provides a high level overview of the system. Based on the hazard analysis and risk assessment, it is figured out what the system is required to do to stay safe. Then the project team identifies, what part of the system will need to be adjusted to take into account the new functionality.
In Functional Safety Concept, safety goals are refined into safety requirements. These safety requirements are then allocated to the appropriate parts of the item's architecture. The functional safety concept looks at the general functionality of the item and does not go into technical details.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

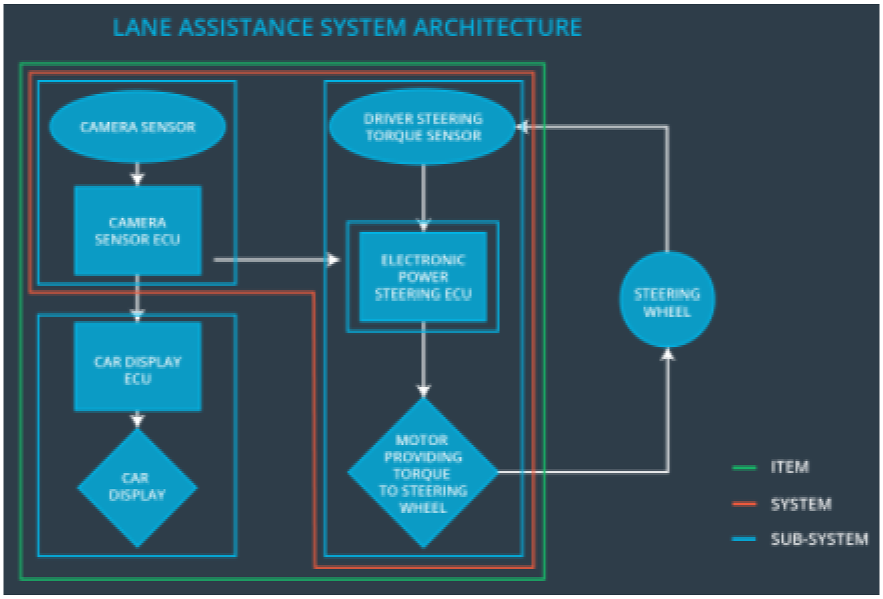
[Instructions:
REQUIRED: Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

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

ID	Safety Goal
Safety_Goal_01	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
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	Sensor responsible for capturing vehicle driving conditions such as surrounding vehicles, obstacles and lane lines.
Camera Sensor ECU	Camera Sensor ECU is a processing unit for perception module. In this project, it is responsible for detecting lane lines and determining ego vehicle's position relative to lane lines.
Car Display	Visual display warning of lane departures, LDW / LKA activation and deactivations.
Car Display ECU	Processing unit responsible for processing information from other item elements and accordingly, display warnings on the car display.

Driver Steering Torque Sensor	Sensor responsible for measuring steering torque that the driver is applying on the steering wheel.
Electronic Power Steering ECU	Processing unit responsible for, - computing appropriate steering torque based on LKA system and steering torque sensor inputs - Oscillatory steering torque that vibrates the steering wheel when the driver drifts away from the lane center.
Motor	Actuator responsible for taking inputs from ECU and then applying requested torque on the steering column

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	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)	NO	The lane keeping

	function shall apply the steering torque when active in order to stay in ego lane		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 keeping items shall ensure that the lane departure oscillating torque amplitude is below max torque amplitude.	C	50 ms	LDW function will be turned 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	50 ms	LDW function will be turned off

* Fault tolerant time interval = diagnostic test interval + fault reaction time + time in safe state before an accident

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	Validate MAX_Torque_Amplitude - high enough to be detected by driver - low enough not to cause loss of steering	Verify that the system turns off, if LDW exceeds MAX_Torque_Amplitude
Functional Safety Requirement	Validate MAX_Torque_Frequency - high enough to be detected by driver	Verify that the system turns off, if LDW exceeds MAX_Torque_Frequency

01-02	- low enough not to cause loss of steering	

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

Lane Keeping Assistance (LKA) Requirements:

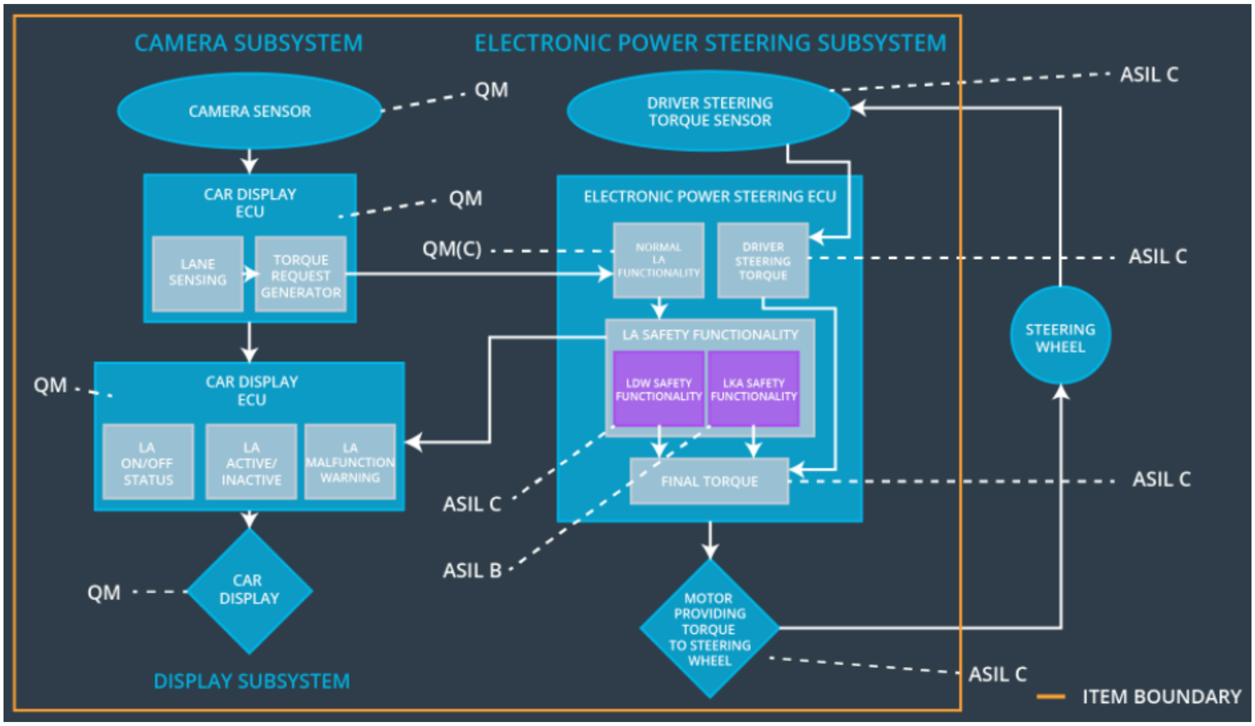
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500 ms	LKA function will be turned off

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	Validate that the Max_Duration chosen prevents driver from taking their hands off the steering	Verify that the system turns off, if LKA exceeds 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.			
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below max torque frequency.	✓		
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is 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	Turn off the functionality	The LDW function applies an oscillating torque with very high torque amplitude / frequency (above limit)	YES	Display a warning on the driver dashboard
WDC-02	Turn off the functionality	The LKA function is not limited in time duration which leads to misuse as an autonomous driving function.	YES	Display a warning on the driver dashboard