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
Mar. 25, 18	0.1	L. Chen	Initial version
Mar. 29, 18	0.2	L. Chen	Minor changes

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 purpose of the functional safety concept is to analyze the item to identify functional safety requirements and allocate them to systems in the item.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

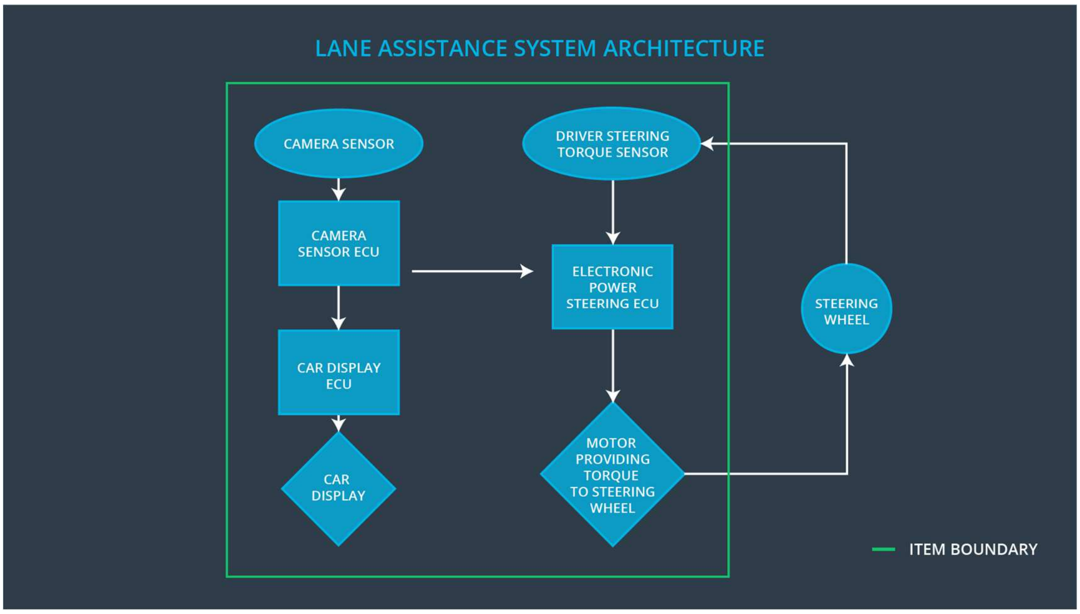
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

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 from the LDW shall be limited
Safety_Goal_02	The lane keeping assistance function should add extra steering torque for a limited amount of time and then stop providing extra torque.

Preliminary Architecture

[Instructions: Provide a preliminary architecture for the lane assistance item. Hint: See


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

Lesson 3: Item Definition]

The preliminary architecture for the lane assistance item is shown in figure.

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	perception of current road environment
Camera Sensor ECU	extract lanes from camera images and estimate current vehicle position in lane
Car Display	display information
Car Display ECU	receive signals from other ECUs and update Car Display
Driver Steering Torque Sensor	measure steering torque of driver
Electronic Power Steering ECU	calculate correct steering torque and update Motor
Motor	provide additional 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 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	Electric Power Steering ECU shall ensure that the torque amplitude provided by LDW shall not exceed max_torque_amplitude	C	50 ms	Off (set vibration torque to zero)
Functional Safety Requirement 01-02	Electric Power Steering ECU shall ensure that the torque frequency provided by LDW shall not exceed max_torque_frequency	C	50 ms	Off (set vibration torque to zero)

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 max_torque_amplitude for LDW	When the torque amplitude exceeds the defined torque amplitude limit, LDW is turned off within 50ms
Functional Safety Requirement 01-02	Define a reasonable limit max_torque_frequency for LDW	When the torque frequency exceeds the defined torque frequency limit, LDW is turned off within 50ms

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

Lane Keeping Assistance (LKA) Requirements:

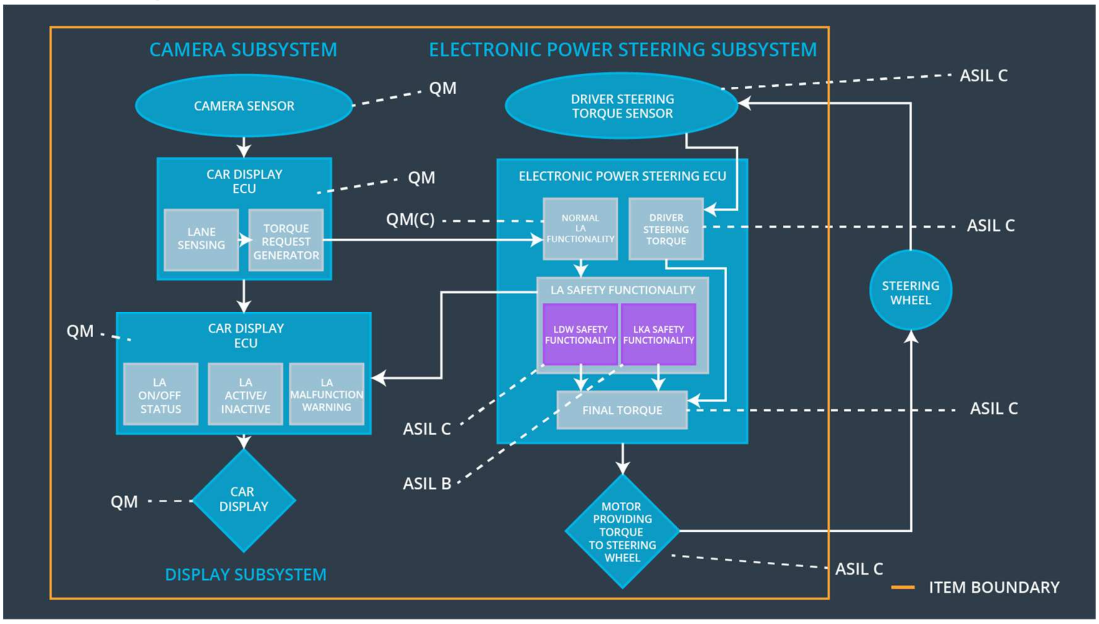
ID	Functional Safety Requirement	A S I L	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	Electric Power Steering ECU shall ensure that the time of LKA torque application is limited to max_duration	B	500 ms	Off (Function turned off)

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	Define a reasonable time limit max_duration to keep drivers taking hands off the wheel	When the hands-off time exceeds the time limit max_duration, LKA is turned off within 500ms

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	Electric Power Steering ECU shall ensure that the torque amplitude provided by LDW shall not exceed max_torque_amplitude	X		
Functional Safety Requirement 01-02	Electric Power Steering ECU shall ensure that the torque frequency provided by LDW shall not exceed max_torque_frequency	X		
Functional Safety Requirement 02-01	Electric Power Steering ECU shall ensure that the time of LKA torque application is limited to 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	Off	If torque amplitude exceeds max_torque_amplitude or torque frequency exceeds max_torque_frequency	yes	Warning light on Car Display

WDC-02	Off	If torque application time exceeds max_duration	yes	Warning light on Car Display