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
4/12/2018	1.0	Joseph Magdy	Initial Release
6/12/2018	1.1	Joseph Magdy	Fix Reviewer Comments

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

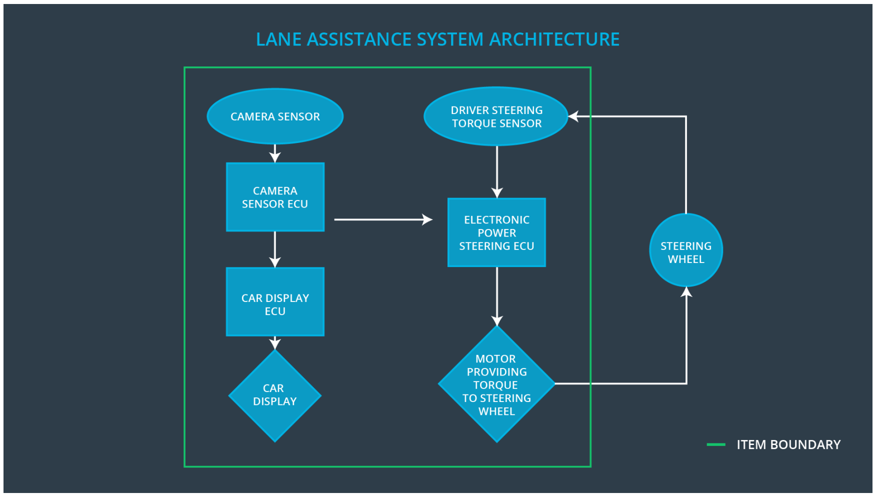
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

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

ID	Safety Goal
Safety_Goal_01	System should have a threshold to limit the torque in such case
Safety_Goal_02	The lane keeping assistance function should only work for a certain amount of time
Safety_Goal_03	Camera sensor should has some sort of lane position compensation during moving on gradient road
Safety_Goal_04	LKA should be activate if the actual steering compared to the previously requested angle is not the same with tolerance during certain time

Preliminary Architecture

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


LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
DRIVER STEERING TORQUE SENSOR
CAMERA SENSOR ECU
ELECTRONIC POWER STEERING ECU
STEERING WHEEL
CAR DISPLAY ECU
CAR DISPLAY
MOTOR PROVIDING TORQUE TO 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	Responsible for reading road image with certain field of view.
Camera Sensor ECU	Responsible for detecting the lanes and when the vehicle is leaving the lane and send the required action to the Car Display and the EPS
Car Display	For displaying instructions to the driver for the lane assistance functions.
Car Display ECU	Processing the requests for the car display by the other ECUs
Driver Steering Torque Sensor	Analyze the driver steering torque
Electronic Power Steering ECU	Responsible for turning the vehicle with the angle requested by the Lane keeping assistance.
Motor	providing 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	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque _Amplitude	C	50 ms	LDW Torque request Amplitude shall be set to zero
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque _Frequency.	C	50 ms	LDW Torque request Amplitude shall be set 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	Validate that we chose a reasonable value. We would need to test how drivers react to different torque amplitudes to prove that we chose an appropriate value.	Verify that the safety requirement is met, by injecting fault torque amplitude crosses the limit and check the lane assistance output is set to zero within the 50 ms which the fault tolerant time interval
Functional Safety Requirement 01-02	Validate that we chose a reasonable value. We would need to test how drivers react to different torque frequencies to prove that we chose an appropriate value.	Verify that the safety requirement is met, by injecting fault torque frequencies crosses the limit and check the lane assistance output is set to zero within the 50 ms which the fault tolerant time interval

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

Lane Keeping Assistance (LKA) Requirements:

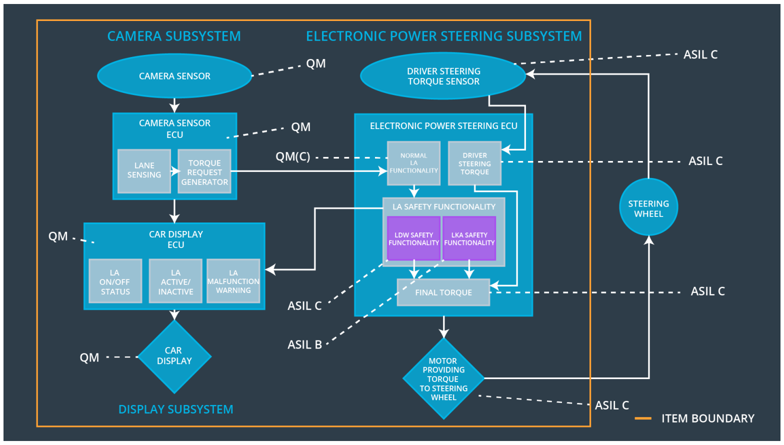
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500ms	LDW Torque request Amplitude shall be set to zero

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 really did dissuade drivers from taking their hands off the wheel	Verify that the system really does turn off if the lane keeping assistance exceeded 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 keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque _Amplitude	**X**		
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque _Frequency.	**X**		
Functional Safety Requirement 02-01	The electronic power steering ECU shall 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	Turn System Off	Malfunction_01	Yes	System Malfunction (LDW Inactive)
WDC-02	Turn System Off	Malfunction_02	Yes	System Malfunction (LDW Inactive)
WDC-03	Turn System Off	Malfunction_03	Yes	Keep Hands on Wheel , function not intended for Autonomous Driving