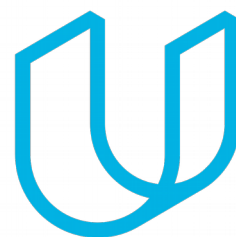# Functional Safety Concept Lane Assistance

Document Version: [Version]
Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
4/17/2018	1.0	Noriaki.H	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

To avoid accidents we'll figure pit which subsystems and elements can be used to meet safety goals.
we will derive functional safety requirements from the safety goals and then add extra functionality to the system diagram. Finally you document your work, a part of functional safety.

Inputs to the Functional Safety Concept
Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscillating steering torque from the lane depature 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
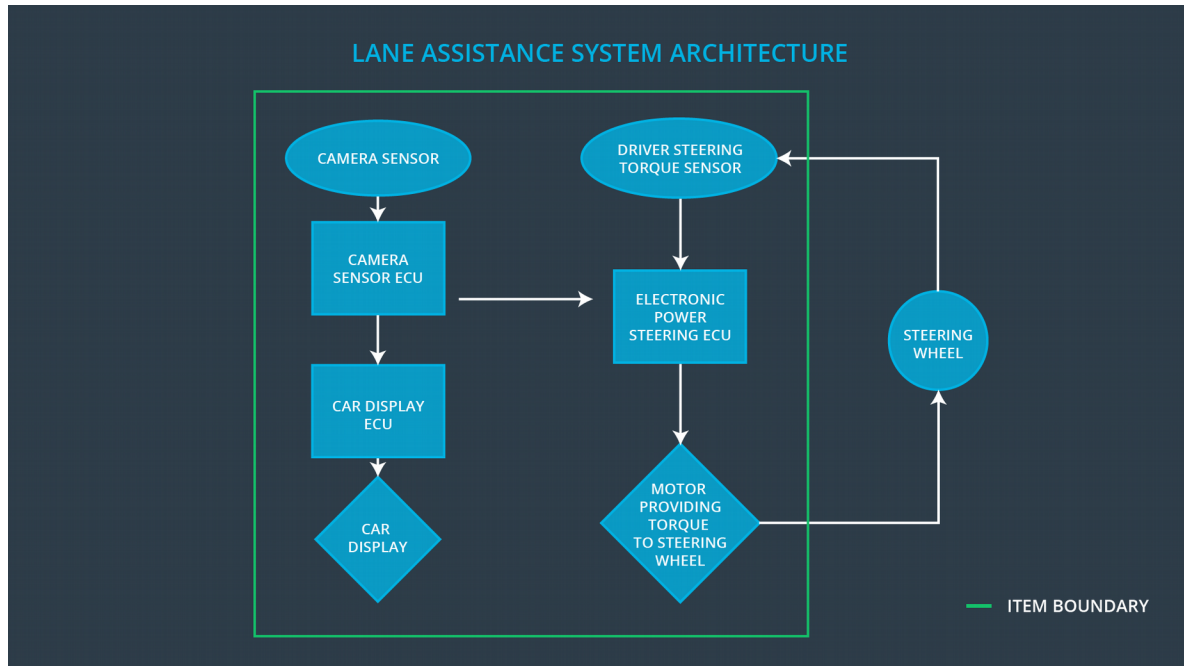
Description of architecture elements

Element	Description
Camera Sensor	The camera sensor reads in images from the road.
Camera Sensor ECU	The Camera sensor ECU identifies when the vehicle has accidentally departed its lane, and sends the appropriate messages to the Car Display ECU and the Electronic Power Steering ECU.
Car Display	Receive to message from Car Display ECU
Car Display ECU	Receive to message from Camera Sensor ECU
Driver Steering Torque Sensor	Receive to message from Steering Wheel and send Electronic Power Steering ECU
Electronic Power Steering ECU	Receive to message from Driver Steering Torque Sensor and Send to Motor Providing torque to steering wheel
Motor	Applies the torque indicated by the Electronic Power Steering ECU 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	The Lane Departure Warning function applies an oscillating torgue 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 torgue 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 shall be time limited, and additional steering torque shall end after a given time interval so the driver cannot misuse the system for autonomous driving.

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	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 depature oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	LDW Torque Request Frequency 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	Test and validate that the Max_Torque_Amplitude chosen really did below Max_Torque_Amplitude	verify that the system really does turn off if exceeded Max_Torque_Amplitude.
Functional Safety Requirement 01-02	Test and validate that the Max_Torque_Amplitude chosen really did below Max_Torque_Frequency	verify that the system really does turn off if exceeded Max_Torque_Frequency.

Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500 ms	Lane Keeping Assistance torque is 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	Test and 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 every exceeded max_duration.

Refinement of the System Architecture
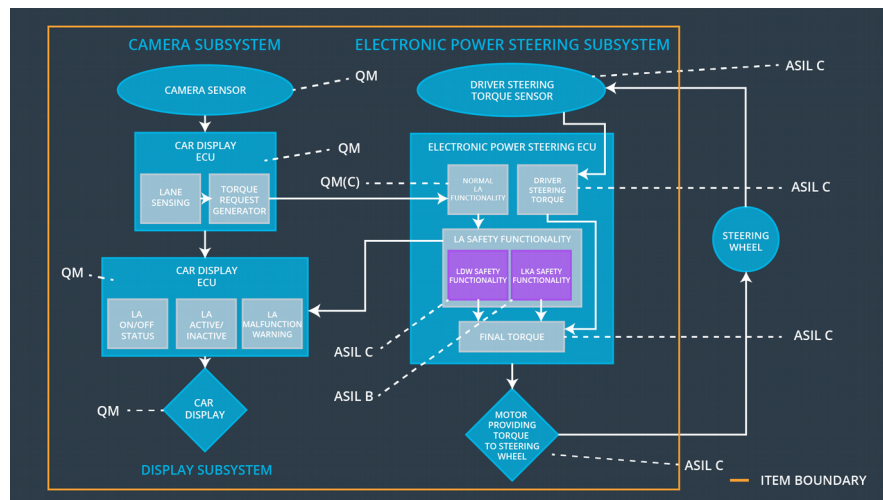
Allocation of Functional Safety Requirements to Architecture Elements

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 depature oscillating torque frequency is below Max_Torque_Frequency	X		
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn System off	Malfunction_01	yes	warning light on the dashboard
WDC-02	Turn System off	Malfunction_02	yes	warning light on the dashboard