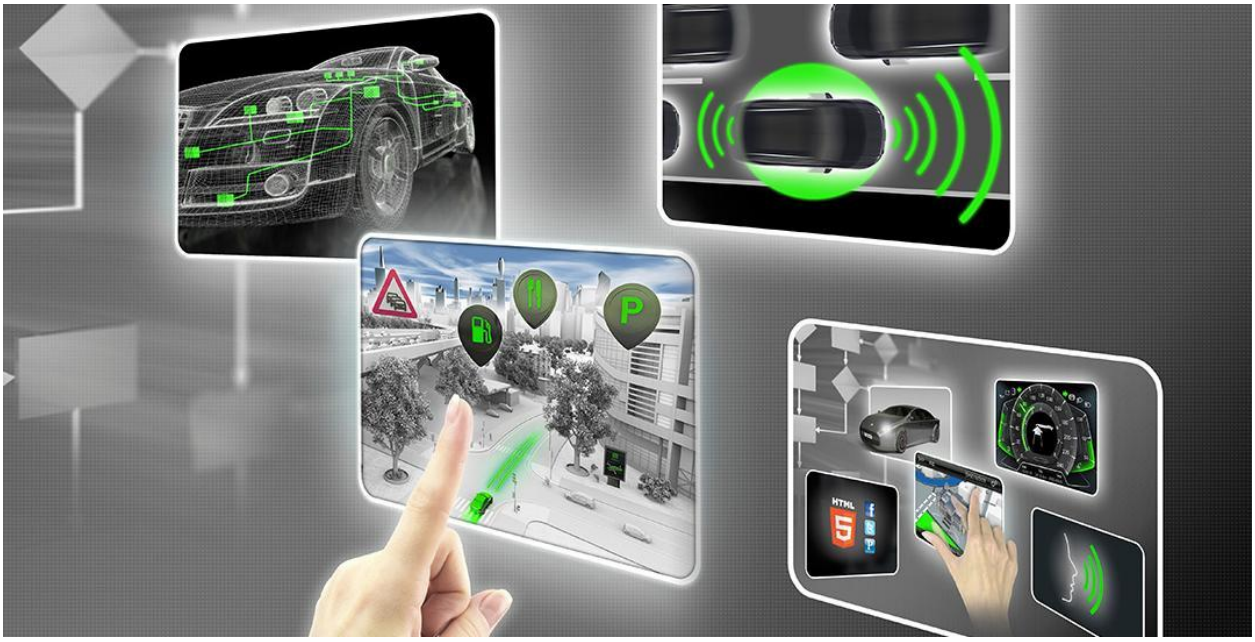
Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
6/7/18	1.0	Yue	First attempt

Table of Contents

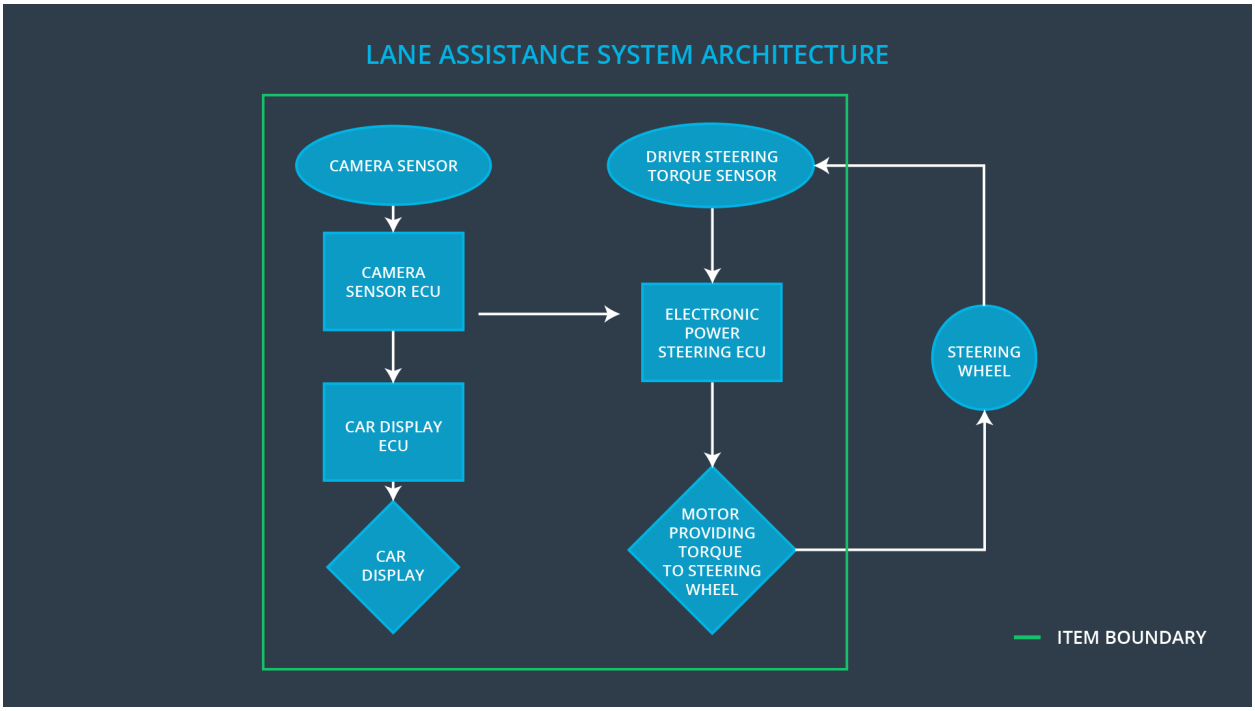
Purpose of the Functional Safety Concept

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscillating torque to the steering wheel from the LDW function shall be limited.
Safety_Goal_02	Lane Keeping Assistance (LKA) function shall apply an oscillating steering torque when driver leaving the steering wheel with both hands
Safety_Goal_03	Lane Keeping Assistance (LKA) function shall apply an oscillating steering torque and deactivated when the sensor cannot detect road
Safety_Goal_04	Lane Keeping Assistance (LKA) function shall apply an oscillating steering torque and deactivated when the road mark is not clear.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Collect road images data.
Camera Sensor ECU	Identifying accidental departure from the road and sending information to the Car Display ECU and the

	Electronic Power Steering ECU.
Car Display	Display information to the driver.
Car Display ECU	Generate messages based on the information from the Camera Sensor ECU.
Driver Steering Torque Sensor	Measure the torque of the steering wheel.
Electronic Power Steering ECU	Ensure lane departure warning oscillating torque amplitude is below max torque amplitude.
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

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 torque amplitude applied by the system is above the limit.
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	The torque frequency applied by the system is above the limit

Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	LATE	The torque is applied too late and did not give the driver enough time to react.

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 Electronic Power Steering ECU shall ensure that the oscillating torque amplitude requested by the LDW function is below Max_Torque_Amplitude	C	50ms	LDW will set the oscillating torque amplitude to 0.
Functional Safety Requirement 01-02	The electronic power steering ECU shall eusure that the lane departure warning oscillating torque frequency is below Max_Torque_Frequency	C	50ms	LDW will set the oscillating torque frequency to 0.

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 is low enough that the driver dose not lost control of the car.	Verify that the system does turn off in time if Max_Torque_Amplitude is exceeded.
Functional Safety Requirement 01-02	Test and validate that the Max_Torque_Frequency chosen is low enough that the driver dose not lost control of the car.	Verify that the system does turn off in time if Max_Torque_Frequency is exceeded.

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

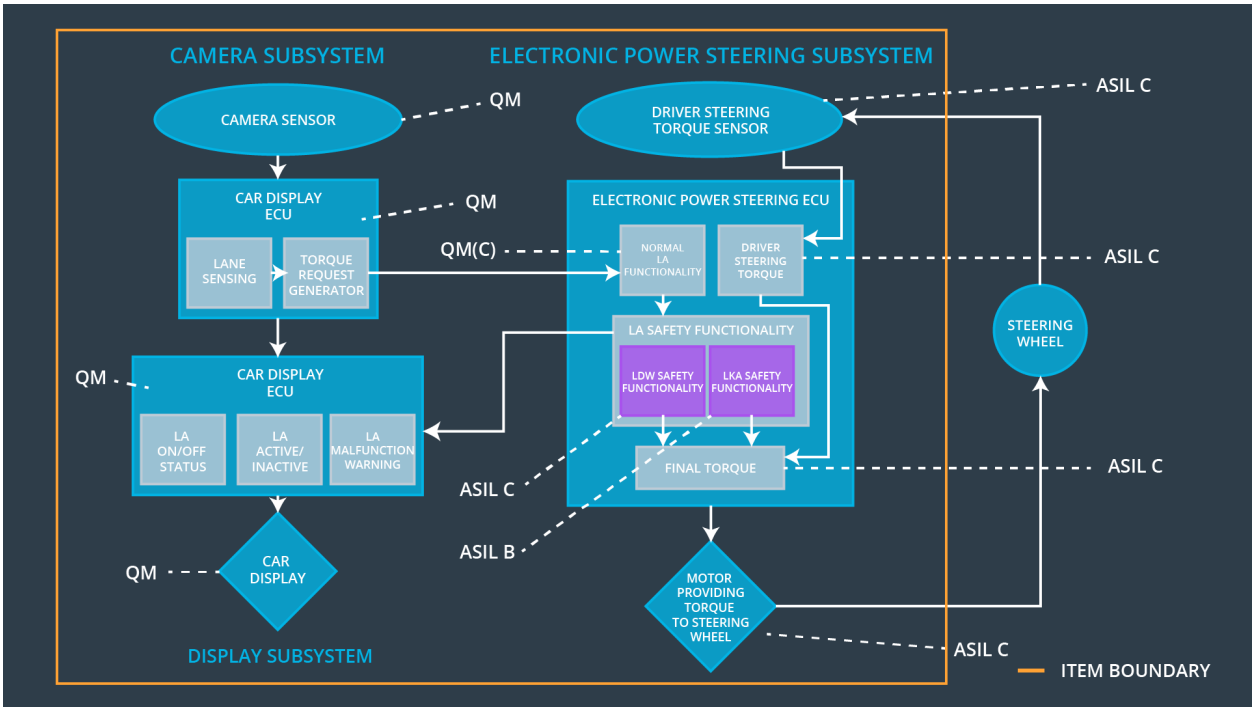
Lane Keeping Assistance (LKA) Requirements:

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	Turn off the system.

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	Verify that the system does turn off and warn the driver if the Max_Duration is exceeded.

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 electronic power steering ECU shall ensure that the lane departure warning oscillation torque amplitude is below Max_Torque_Frequency	**X**		
Functional Safety Requirement 01-02	The electronic power steering ECU shall eusure that the lane departure warning oscillating torque frequency is below Max_Torque_Frequency	**X**		
Functional Safety Requirement	The electronic power steering ECU shall ensure that the lane keeping assistance torque is	**X**		

02-01	applied within Max_Duration			

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the torque and warning.	Malfunction_01 Malfunction_02	YES	Warning light on dashboard with warning noise.
WDC-02	Turn system off and warning.	Malfunction_03	YES	Warning light on dashboard with warning noise.