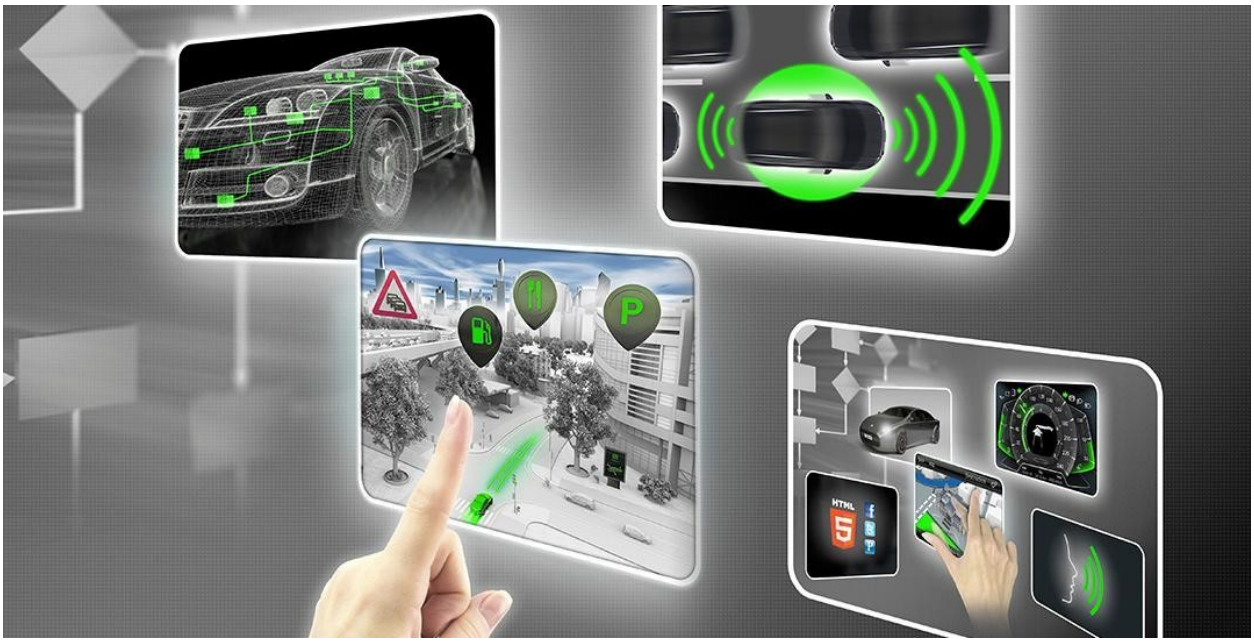
Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [1.0]



Document history

Date	Version	Editor	Description
2019-04-18	1.0	Justin Simerly	First submission.

Table of Contents

Purpose of the Functional Safety Concept

The functional safety concept looks at the general functionality of the item, identifying new requirements and allocating these requirements to system diagrams.

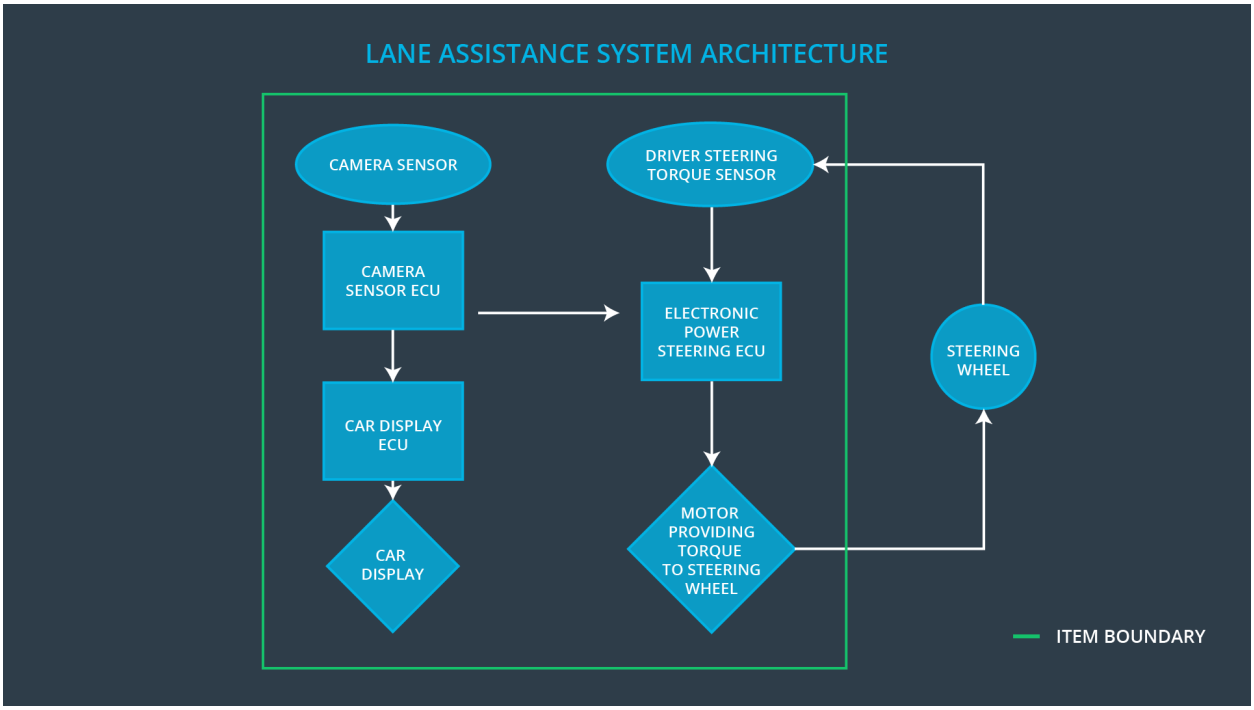
Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscillating steering torque from the lane 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 timer interval so that the driver can not misuse the system for autonomous driving.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Provides the camera input.
Camera Sensor ECU	Derives lanes from the camera sensor and requests the desired steering wheel torque.
Car Display	Controls the output of the car dashboard.
Car Display ECU	Outputs a warning light when the Lane Departure Warning function is activated.
Driver Steering Torque Sensor	Measures the torque applied to the steering wheel.
Electronic Power Steering ECU	Calculates the resulting torque to apply to the steering wheel based on the desired and current torque.
Motor	Turns 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 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

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 lane departure warning oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 mS	The torque request from the lane keeping assistance will be set to 0.
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency is below Max_Torque_Frequency.	C	50 mS	The torque request from the lane keeping assistance will be set 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 how drivers react to the chosen Max_Torque_Amplitude.	A software test that sets the torque amplitude above Max_Torque_Amplitude and ensures the lane assistance output is set to 0 within the fault tolerant time interval.
Functional Safety Requirement 01-02	Test how drivers react to the chosen Max_Torque_Frequency.	A software test that sets the torque frequency above Max_Torque_Frequency and ensures the lane assistance output is set to 0 within the fault tolerant time interval.

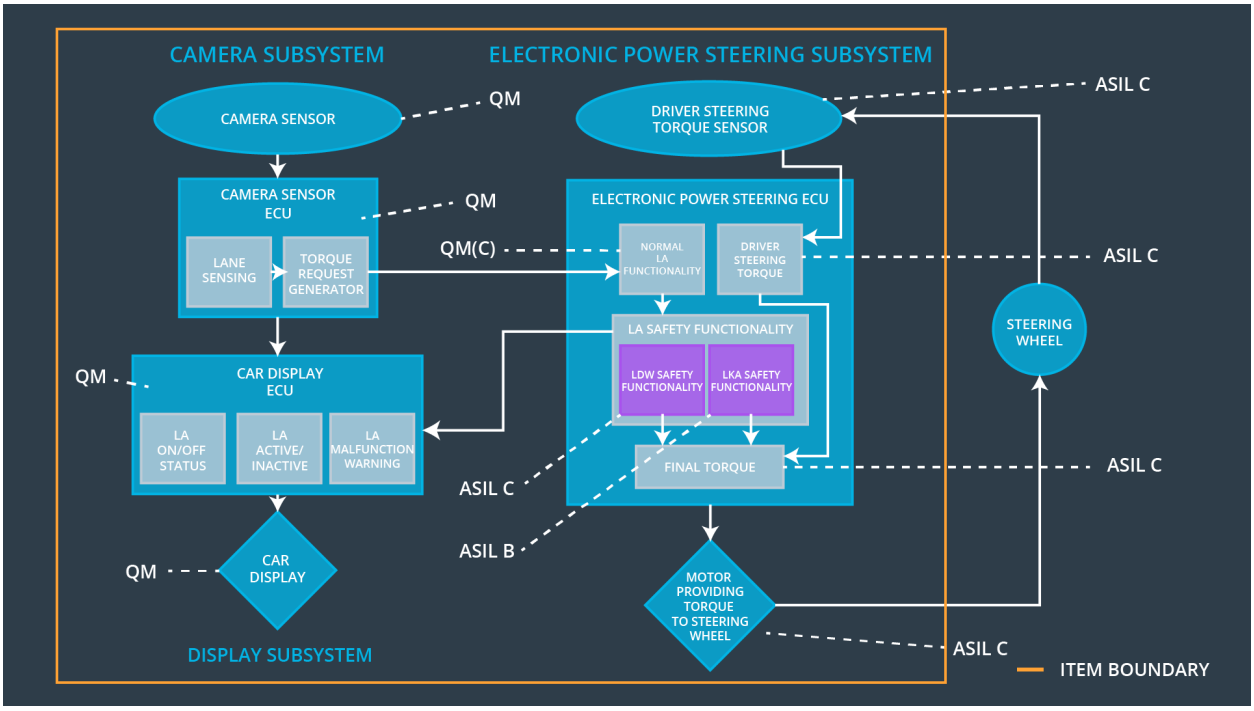
Lane Keeping Assistance (LKA) Requirements:

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	The torque request from the lane keeping assistance will be set to 0.

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 that the Max_Duration did dissuade drivers from taking their hands off the wheel.	Verify the system turns off if the lane keeping assistance exceeds 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 electronic power steering ECU shall ensure that the lane departure warning oscillating torque amplitude is below Max_Torque_Amplitude.	**X**		
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency 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

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the Lane Departure Warning functionality.	The lane departure warning function applies an oscillating torque with very high torque amplitude (above limit).	yes	Car Display shows a Lane Assist Malfunction Warning.
WDC-02	Turn off the Lane Keeping Assistance functionality.	The lane keeping assistance function is not limited in time duration which leads to misuse as an autonomous driving function.	yes	Car Display shows a Lane Assist Malfunction Warning.