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
8/25/2018	Ver0.1	Jun Imamura	First Attempt

Table of Contents

Purpose of the Functional Safety Concept

Functional safety concept is a documentation activity to identify which subsystem has the risk of hazardous situation. At first, examine the safety goals and list up functional safety requirements. Then, allocate them to respective subsystems accordingly.

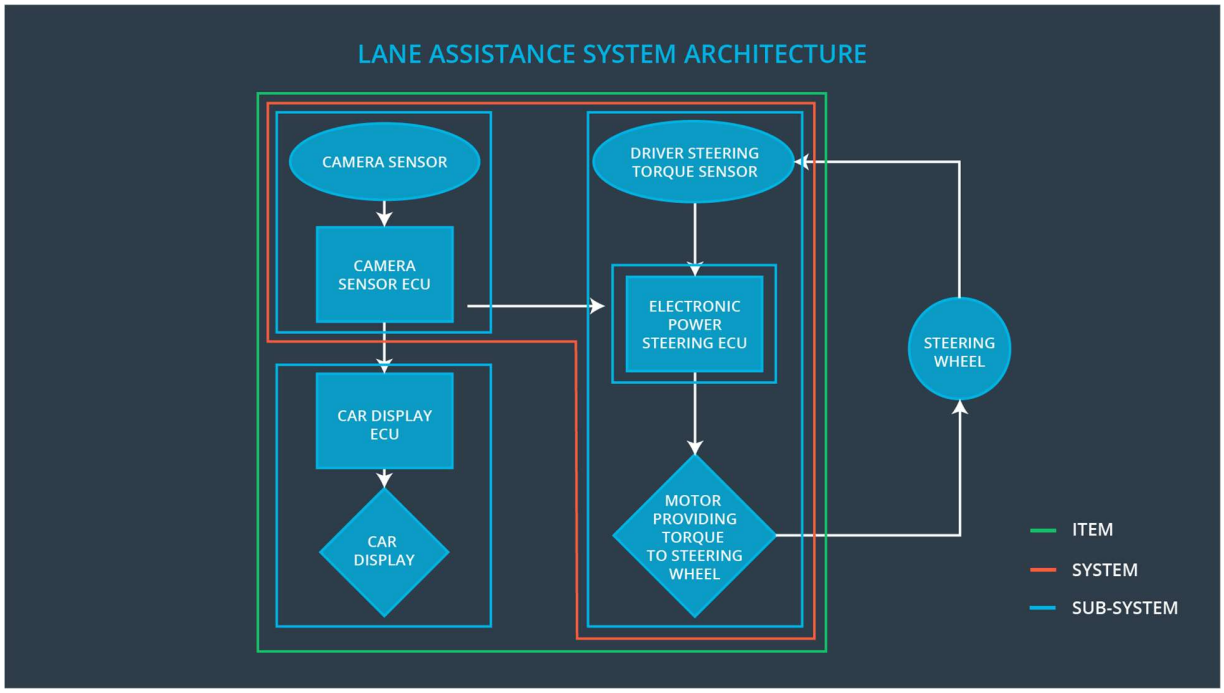
Inputs to the Functional Safety Concept

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 additional steering torque shall end after a given time interval so the driver cannot misuse the system for autonomous driving.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Capture the images ahead of the vehicle and provide them to the Camera Sensor ECU
Camera Sensor ECU	Process the provided sensor raw values and detect / calculate the position of the car on the road. Then request a desirable torque to the electronic power steering ECU.

Car Display	Provide both activation status and operating status of the lane assistance functionality.
Car Display ECU	Receive activation status an operating status from the camera sensor ECU and drive indicator in the car display to show received status to the driver.
Driver Steering Torque Sensor	Measure the torque applied to the steering wheel by the driver.
Electronic Power Steering ECU	Receive currently applied torque from driving steering torque sensor and desired torque from camera sensor ECU respectively. Then decide and request to apply necessary torque.
Motor	Apply the torque which is requested by 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 torque with very high torque amplitude (above limit)
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering	MORE	The lane departure warning function applies an oscillating torque with very high

	torque to provide the driver a haptic feedback		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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Torque amplitude request set to zero.
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is blow Max_Torque_Frequency	C	50ms	Torque amplitude request 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 Max_Torque_Amplitude becomes not too high so that the driver doesn't lose control of steering.	Verify the system does turn off in time if the strength of the torque exceeds Max_Torque_Amplitude.
Functional Safety Requirement 01-02	Validate Max_Torque_Frequency becomes not too high so that the driver doesn't lose control of steering.	Verify the system does turn off in time if the frequency of the torque exceeds Max_Torque_Frequency.

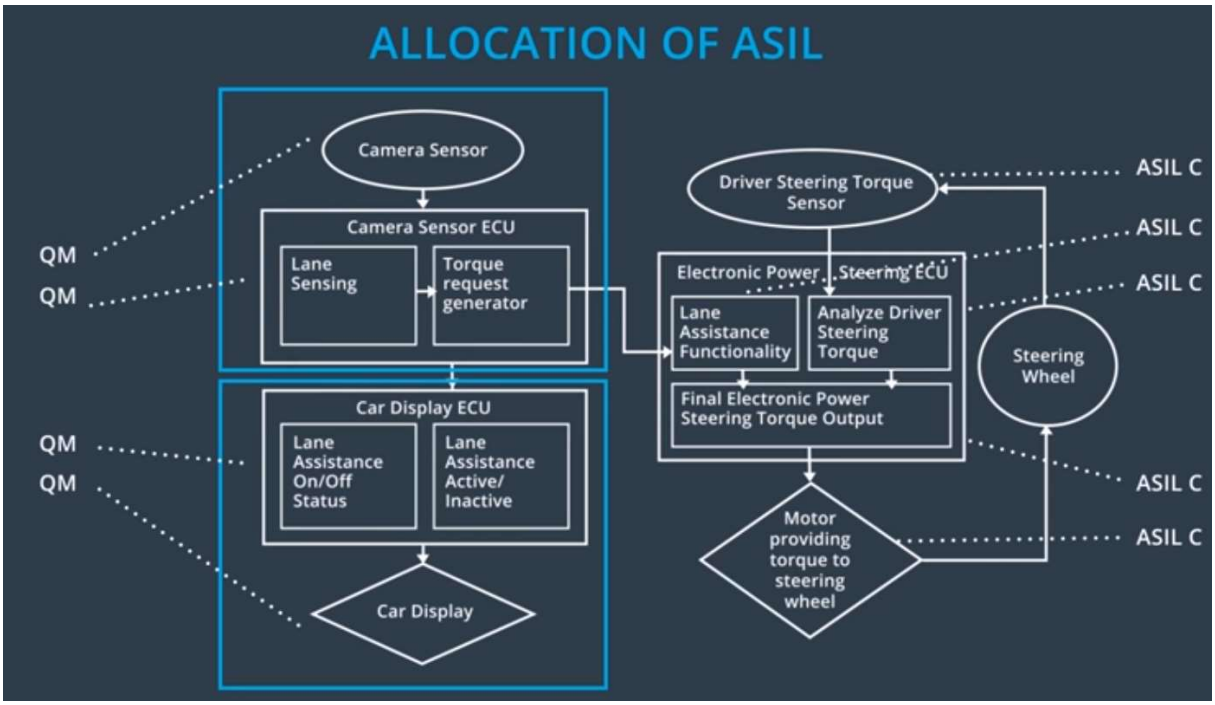
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500ms	System 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	Test and validate that the electric power steering stop providing assistant torque to avoid the driver misusing the functionality as the autonomous driving.	

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 departure oscillating torque frequency is blow Max_Torque_Frequency	**x**		
Functional Safety Requirement	The electronic power steering ECU shall ensure that the lane	**x**		

02-01	keeping assistance torque is applied for only Max_Duration.			

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	System turned off	Malfunction_01 Malfunction_02	Yes	Warning indication on the car display
WDC-02	System turned off	Malfunction_03	Yes	Warning indication of the car display