Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
04-14-2018	0.1	Pablo	Purpose, Inputs
04-21-2018	1.0	Pablo	Finish document

Table of Contents

Purpose of the Functional Safety Concept

The purpose of the functional safety concept is to define the high level safety requirements and allocate them to the relevant parts of the system diagram, for the Lane Assistant system item.

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 time interval so that the driver cannot misuse the system for autonomous driving

Preliminary Architecture

Figure 1 shows the preliminary architeture for the lane assistance system.

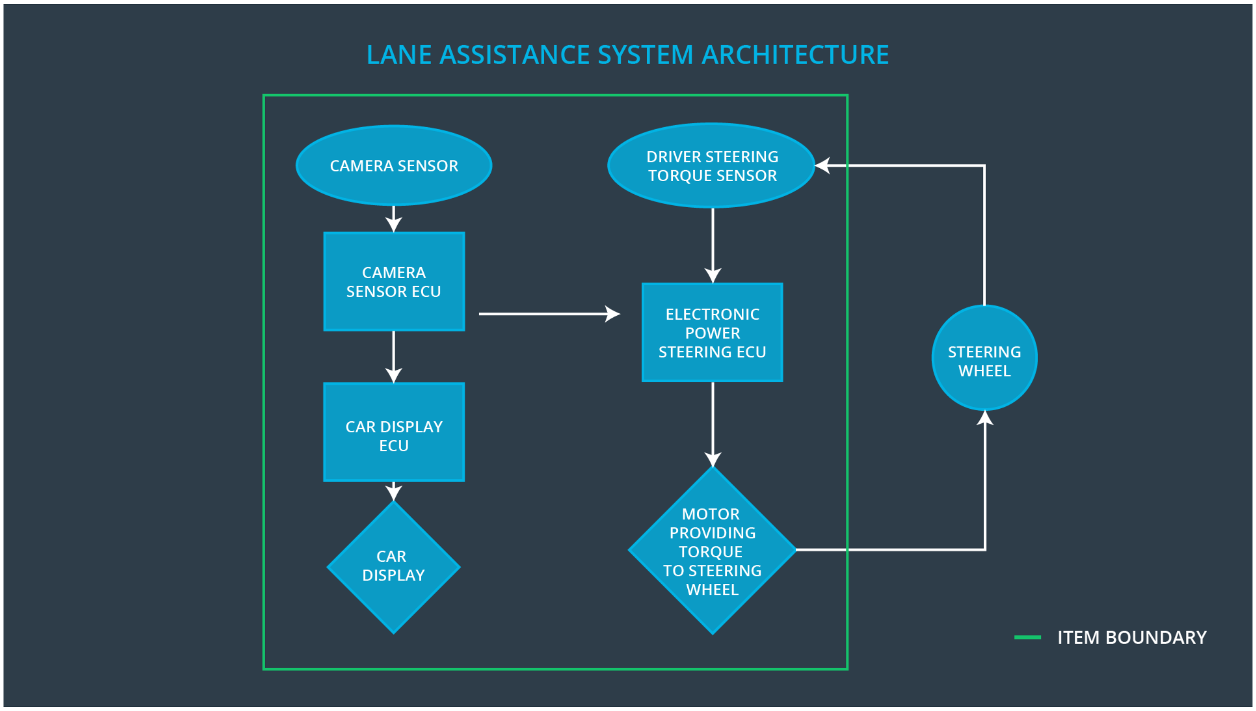
LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
CAMERA SENSOR ECU
CAR DISPLAY ECU
CAR DISPLAY
DRIVER STEERING TORQUE SENSOR
ELECTRONIC POWER STEERING ECU
MOTOR PROVIDING TORQUE TO STEERING WHEEL
STEERING WHEEL
ITEM BOUNDARY

Figure 1: Lane Assistance System Architecture

Description of architecture elements

Element	Description
Camera Sensor	Captures road images and transmits them to the Camera Sensor ECU
Camera Sensor ECU	Based on the received images, detects lane lines and determines when the vehicle leaves the lane by mistake. Sends departure warning signal to the Car Display ECU. Send estimated torque required to the Electronic Power Steering ECU.

Car Display	Displays warnings related to the Lane Departure Status.
Car Display ECU	Processes Lane Departure Warning signals from Camera Sensor ECU and transmits display signal and information to the Car Display.
Driver Steering Torque Sensor	Measures the torque applied to the steering wheel. Sends torque signal to the Electronic Power Steering ECU.
Electronic Power Steering ECU	Adjusts the torque required to correct the vehicle trajectory based on the driver steering torque sensor and the camera sensor ECU.
Motor	Applies the torque required 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 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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Vibration torque is zero
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque is below Max_Torque_Frequency	C	50 ms	Vibration torque is 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 we chose a reasonable Max_Torque_Amplitude value for drivers	If Torque_Amplitude >= Max_Torque_Amplitude, the lane assistance output is set to zero within the 50 ms fault tolerant time interval
Functional Safety Requirement 01-02	Test and Validate that we chose a reasonable Max_Torque_Frequency value for drivers	If Torque_Frequency >= Max_Torque_Frequency, the lane assistance output is set to zero within the 50 ms 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	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.	The system does turn off if the lane keeping assistance exceeded Max_Duration

Refinement of the System Architecture

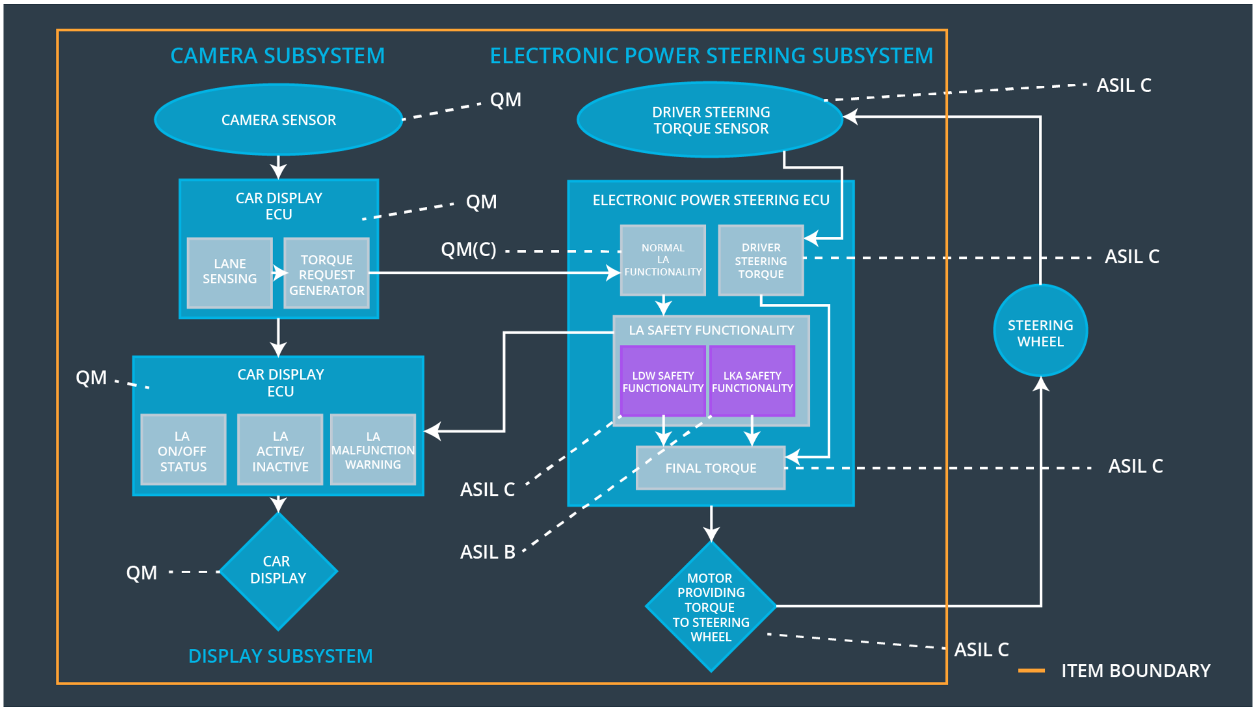

Figure 2: System ASIL Levels

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 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	The torque request from the lane keeping assistance will be set to zero.	Malfunction_01, Malfunction_02	Yes	Warning light on the dashboard when the system malfunctions
WDC-02	The torque request from the lane keeping assistance will be set to zero.	Malfunction_03	Yes	Warning light on the dashboard when the system malfunctions