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
5 September 2017	1.0	Ed Venator	Initial Submission

Table of Contents

Purpose of the Functional Safety Concept

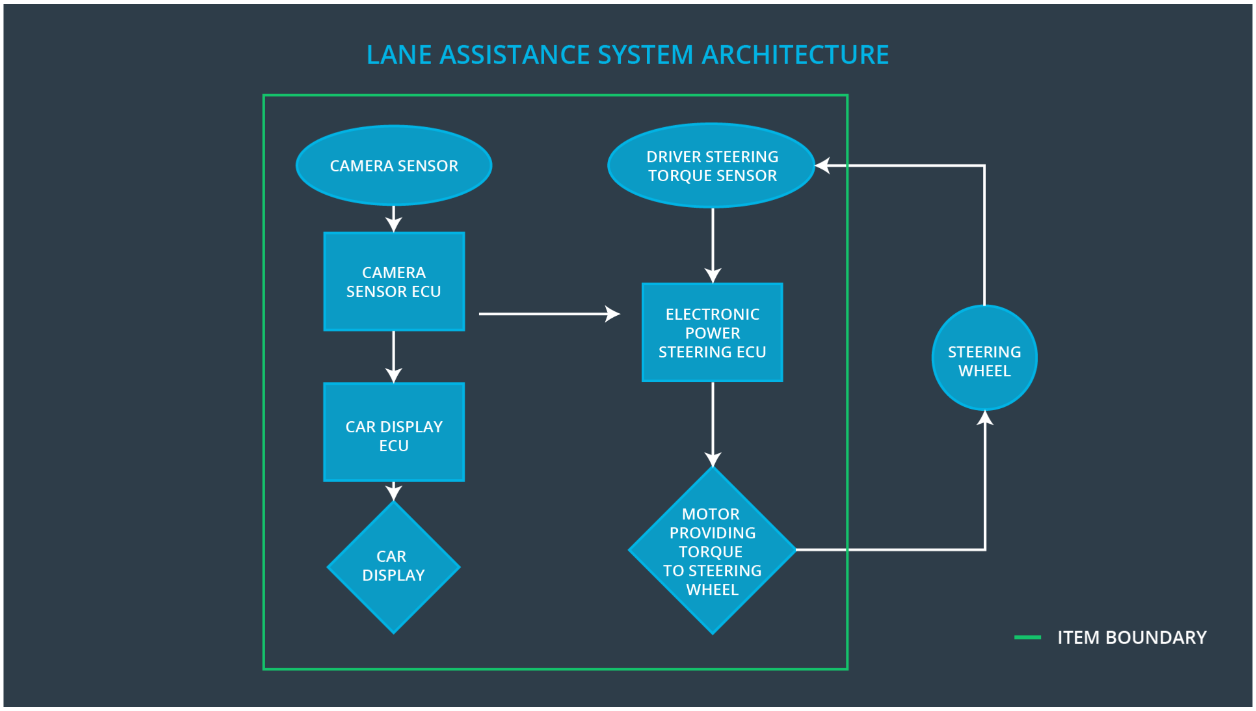
The Functional Safety Concept is an important part of reducing the risk of the system to acceptable levels. This document defines the architecture and the safety requirements. It also allocates those safety requirements to the various parts of the architecture. In the process, the Functional Safety Concept defines parameters for the requirements, such as ASIL, fault tolerant time interval, and safe states. These parameters define the requirements for the system's design and operation. The Functional Safety Concept approaches these tasks from a high level; more in-depth technical details, such as the actual implementation of the requirements, is defined in the Technical 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 steering torque delivered to the steering wheel by the LDW function shall be limited.
Safety_Goal_02	The lane keeping assistance function shall be time-limited such that the additional steering torque shall end after a given time interval so that the driver cannot misuse the system for autonomous driving.
Safety_Goal_03	The steering torque delivered to the steering wheel by the LKA function shall be limited.

Preliminary Architecture


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

Description of architecture elements

Element	Description
Camera Sensor	Captures imagery of the road in front of the vehicle.
Camera Sensor ECU	Processes camera imagery to detect the car's position in the ego lane. Requests torque from the Electronic Power Steering ECU.
Car Display	Displays the status of the LDW and LKA functions.
Car Display ECU	Tracks the status of the LDW and LKA functions and controls the Car Display.
Driver Steering Torque Sensor	Senses the torque applied to the steering wheel by the driver.
Electronic Power Steering ECU	Handles torque requests from the Camera Sensor ECU. Controls the Motor to deliver torque to the steering wheel, using the Driver Steering Torque Sensor as feedback.
Motor	Provides torque to the steering wheel; controlled by the Electronic Power Steering ECU.

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 LDW applies an oscillating torque with very high 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 LDW applies an oscillating torque with very high 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 LKA function is not time-limited, allowing its 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 is below Max_Torque_Ampliltude.	C	50ms	LDW disabled (output torque zero)
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque is below Max_Torque_Frequency.	C	50ms	LDW disabled (output torque 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	With driver testing, confirm that the value of Max_Torque_Amplitude is low enough that drivers can maintain control of the vehicle.	Verify that when the torque exceeds Max_Torque_Amplitude, the LDW is disabled (torque to zero) within 50ms.
Functional Safety Requirement 01-02	With driver testing, confirm that the value of Max_Torque_Frequency is low enough that drivers can maintain control of the vehicle.	Verify that when the torque exceeds Max_Torque_Frequency, the LDW is disabled (torque to zero) within 50ms.

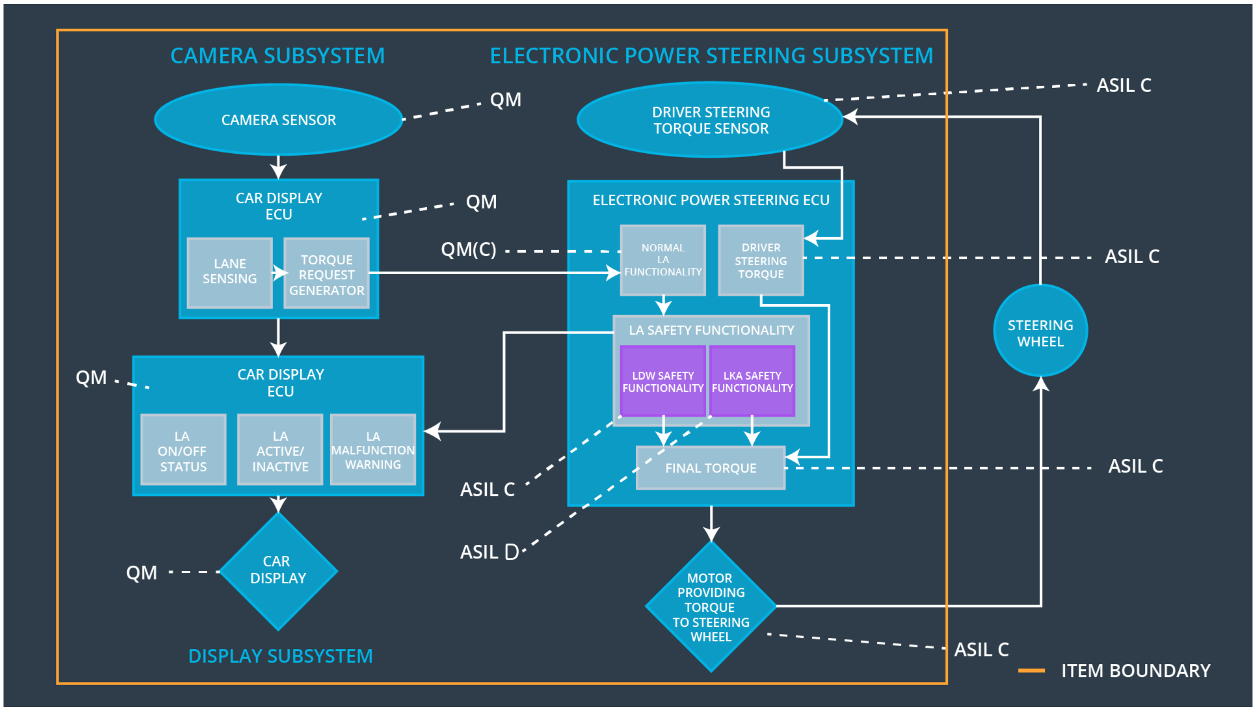
Lane Keeping Assistance (LKA) Requirements:

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.	C	500ms	LKA disabled (output torque zero)
Functional Safety Requirement 03-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is below Max_Torque_Magnitude.	D	50ms	LKA disabled (output torque 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	With driver testing, confirm that the Max_Duration does cause drivers to keep their hands on the steering wheel.	Verify that the system does turn off (torque to zero) after Max_Duration.
Functional Safety Requirement 03-01	With driver testing, confirm that Max_Torque_Magnitude is low enough that drivers can override the LKA.	Verify that the system does turn off within (torque to zero) 50ms if the torque exceeds Max_Torque_Magnitude.

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 is below Max_Torque_Ampliltude.	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		
Functional Safety Requirement 03-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is below Max_Torque_Magnitude.	X		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW	The LDW applies an oscillating torque with very high amplitude (above limit).	Yes	Display shows warning light
WDC-02	Turn off LKA	The LDW applies an oscillating torque with very high frequency (above limit).	Yes	Display shows warning light
WDC-03	Turn off LKA	The LKA function is not time-limited, allowing its misuse as an autonomous driving function.	Yes	Display shows warning light