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
11/2/17	1.0	Nicholas Moellers	First submission

Table of Contents

Purpose of the Functional Safety Concept

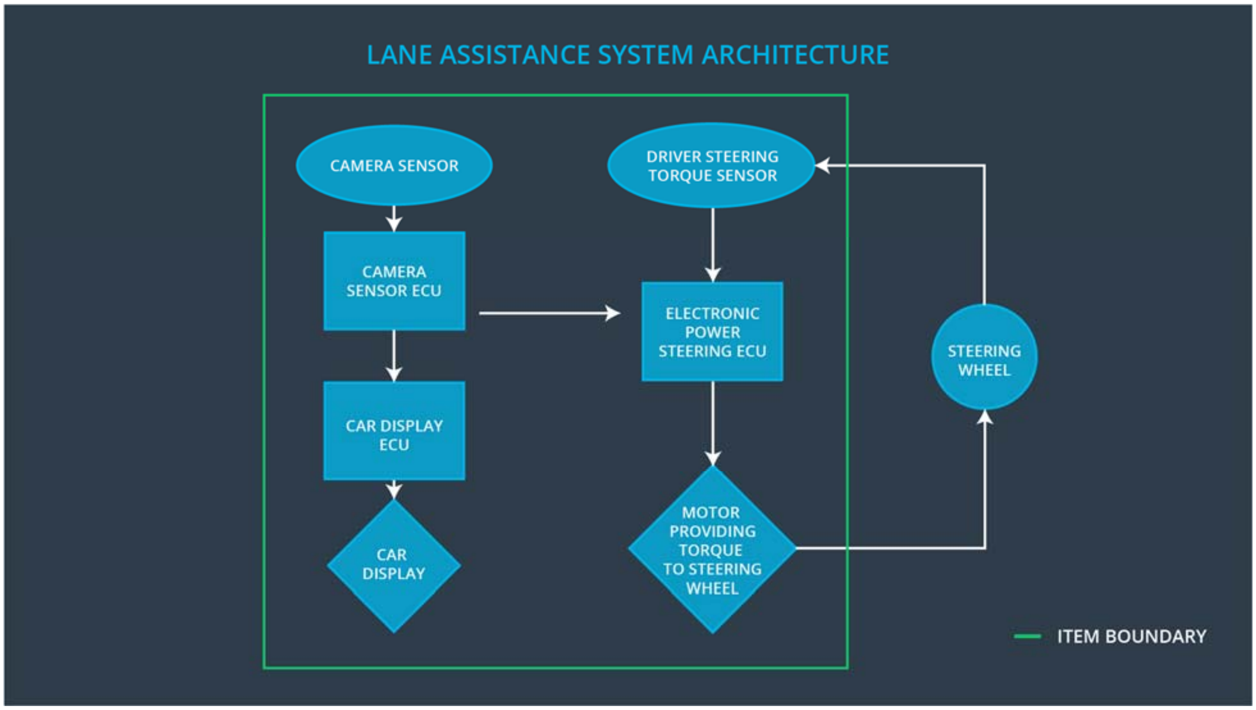
The purpose of this document is to refine the safety goals into functional safety requirements and allocate those requirements to the appropriate parts of the system diagram. Specifically, we will look at the ASIL levels of components, the fault tolerant time intervals, and the safe state. This document will look at safety from a high level; the next document will go into the technical details.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscillating torque feedback from the lane departure warning function shall be limited in both frequency and amplitude.
Safety_Goal_02	The lane keeping assistance function shall be time limited.
Safety_Goal_03	The lane keeping assistance function shall not activate unless the driver has explicitly enabled the feature.
Safety_Goal_04	The lane keeping assistance function shall deactivate when the lane lanes are undetectable.

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	Responsible for providing image data about the lane lines to the Camera Sensor ECU
Camera Sensor ECU	Responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake
Car Display	Responsible for displaying the image date from the Car Display ECU
Car Display ECU	Responsible for calculating the appropriate image to send to the Car Display, based on the determination of the Camera Sensor ECU
Driver Steering Torque Sensor	Responsible for measure the torque on the Steering Wheel provided by the driver
Electronic Power Steering ECU	Responsible for calculating the appropriate amount of torque for the motor to apply based on data from the Driver Steering Torque Sensor and from the Camera Sensor ECU
Motor	Responsible for applying torque to the Steering Wheel as determined 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	The lane departure warning is giving MORE torque than what is safe	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	The lane departure warning is giving MORE torque than what is safe	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	The lane keeping assistance has NO time limit	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	A S I L	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	Set vibration torque to zero
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 mS	Set vibration torque 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	The Max_Torque_Amplitude is sufficiently small that drivers really can keep control of the vehicle	the system really does turn off if the lane departure warning vibrations every exceeded Max_Torque_Amplitude
Functional Safety Requirement 01-02	The Max_Torque_Frequency is sufficiently small that drivers really can keep control of the vehicle	the system really does turn off if the lane keeping assistance ever exceeded Max_Torque_Frequency

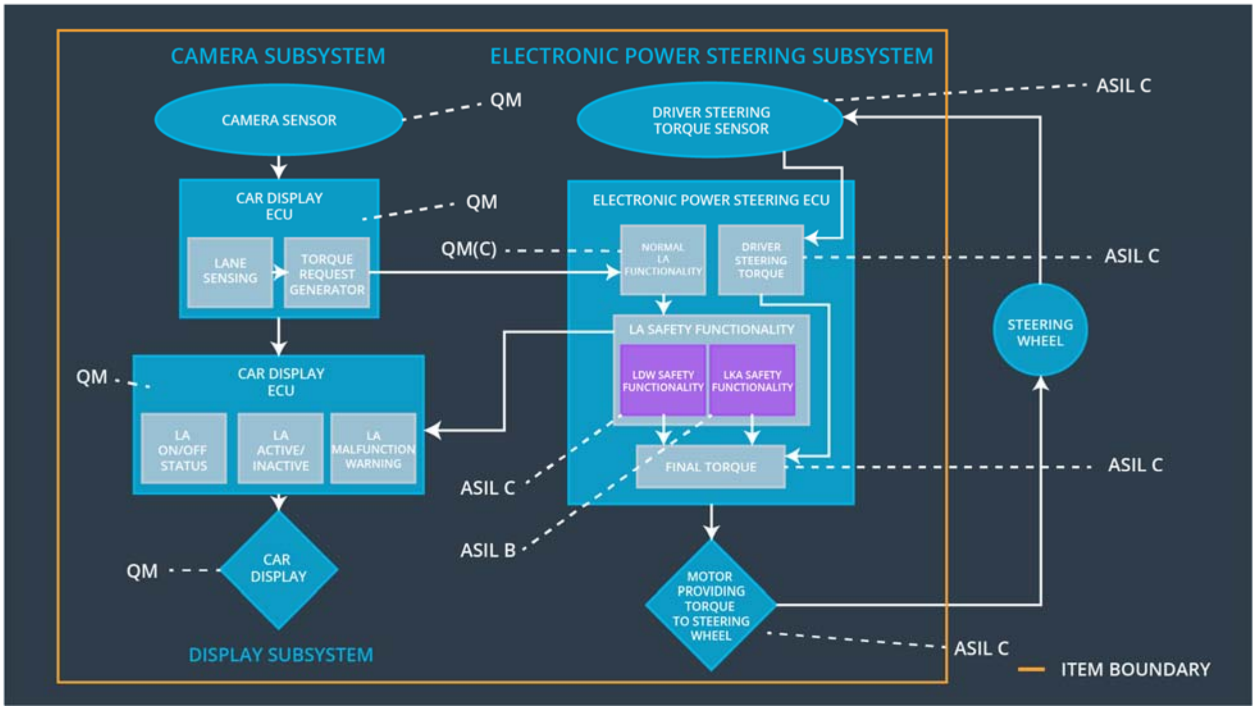
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	A S I L	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500 mS	Lane keeping item is disabled

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	the max_duration chosen really did dissuade drivers from taking their hands off the wheel	the system really does turn off if the lane keeping assistance ever exceeded 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	The Electronic Power Steering ECU shall ensure that the lane	X		

01-01	departure oscillating torque amplitude is below Max_Torque_Amplitude			
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the lane departure 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	Lane keeping assistance mode is disabled	Lane keeping assistance torque has been applied for some time greater than Max_Duration	Yes	Lane keeping mode has been disabled because the functionality is not meant for autonomous driving, and the driver maintains responsibility for the safe operation of the vehicle.
WDC-02	Lane departure warning mode is disabled	The departure warning vibrations have exceeded either Max_Torque_Amplitude or Max_Torque_Frequency	Yes	Lane departure warning mode is disabled to ensure that the driver can maintain control of the vehicle