Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description
6/23/19	1.0	R.Crane	Initial draft of functional safety concept

Table of Contents

Document history

Table of Contents

Purpose of the Functional Safety Concept

Inputs to the Functional Safety Analysis
- Safety goals from the Hazard Analysis and Risk Assessment
- Preliminary Architecture
  - Description of architecture elements

Functional Safety Concept
- Functional Safety Analysis
- Functional Safety Requirements
- Refinement of the System Architecture
- Allocation of Functional Safety Requirements to Architecture Elements
- Warning and Degradation Concept

Purpose of the Functional Safety Concept

This document describes the project's functional safety requirements – requirements derived the high-level functional safety goals and then allocated to an item in the system architecture.

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 function shall be limited in time and additional steering torque shall end after given interval to prevent misuse.

Preliminary Architecture

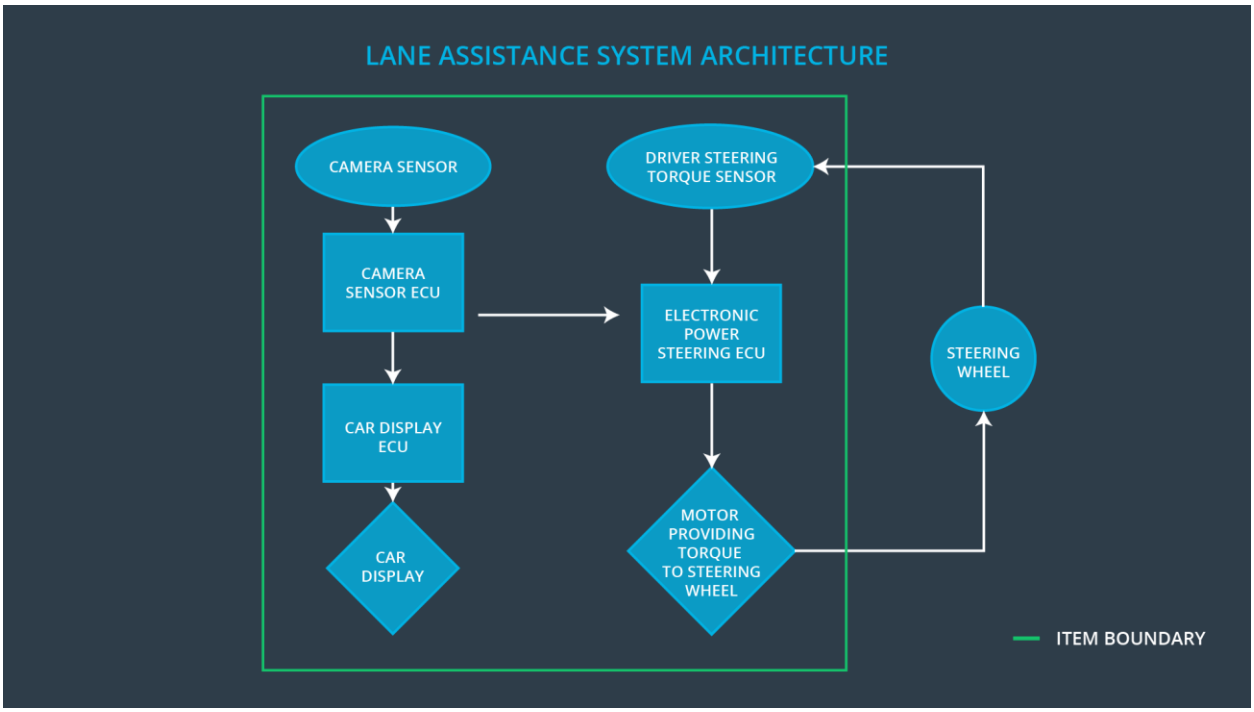

Figure 1. Lane Assistance Architecture.

The Lane Assistance System consists of three subsystems:

- The Camera system
- The Electronic Power Steering system
- The Car Display system

Description of architecture elements

Element	Description
Camera Sensor	Creates and transmits imagery data of the road surface to an extent that lane lines are visible.
Camera Sensor ECU	Processes imagery to detect lane lines and determine vehicle lateral position in the lane.
Car Display	Display visual indication of system readiness and activation. Provide an interface for disabling system.
Car Display ECU	Process the control signals from the display and dispatch commands to appropriate controls for enabling/disabling.
Driver Steering Torque Sensor	Determines the amount of steering input being provided by driver.
Electronic Power Steering ECU	From position information and control signals, determine to apply torque on the steering wheel for lane departure warning and lane keeping assistance.
Motor	Create the physical torque when signalled

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	MORE	The lane departure warning function applies an oscillating

	an oscillating steering torque to provide the driver a haptic feedback		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

[Instructions: Fill in the functional safety requirements for the lane departure warning]

Lane Departure Warning (LDW) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The EPS ECU shall ensure that the lane departure oscillating torque amplitude is below MAX_TORQUE_AMPLITUDE.	C	50ms	LDW shall set torque amplitude to 0.
Functional Safety Requirement 01-02	The EPS ECU shall ensure that the lane departure oscillating torque amplitude is below MAX_TORQUE_FREQUENCY.	C	50ms	LDW shall set torque frequency to 0 Hz.

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 that torque values up to MAX_TORQUE_AMPLITUDE allow continued safe operation of vehicle.	Verify that a torque in excess of MAX_TORQUE_AMPLITUDE causes amplitude to change to 0.
Functional Safety Requirement 01-02	Validate that torque values up to MAX_TORQUE_FREQUENCY allow continued safe operation of vehicle.	Verify that a torque in excess of MAX_TORQUE_FREQUENCY causes frequency to change to zero.

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	LKA shall apply 0 additional torque to power steering.

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	Validate that limiting LKA application to MAX_DURATION dissuades drivers from treating system as an autonomous system.	Verify that continued system operation past MAX_DURATION causes system to stop applying additional torque to steering.

Refinement of the System Architecture

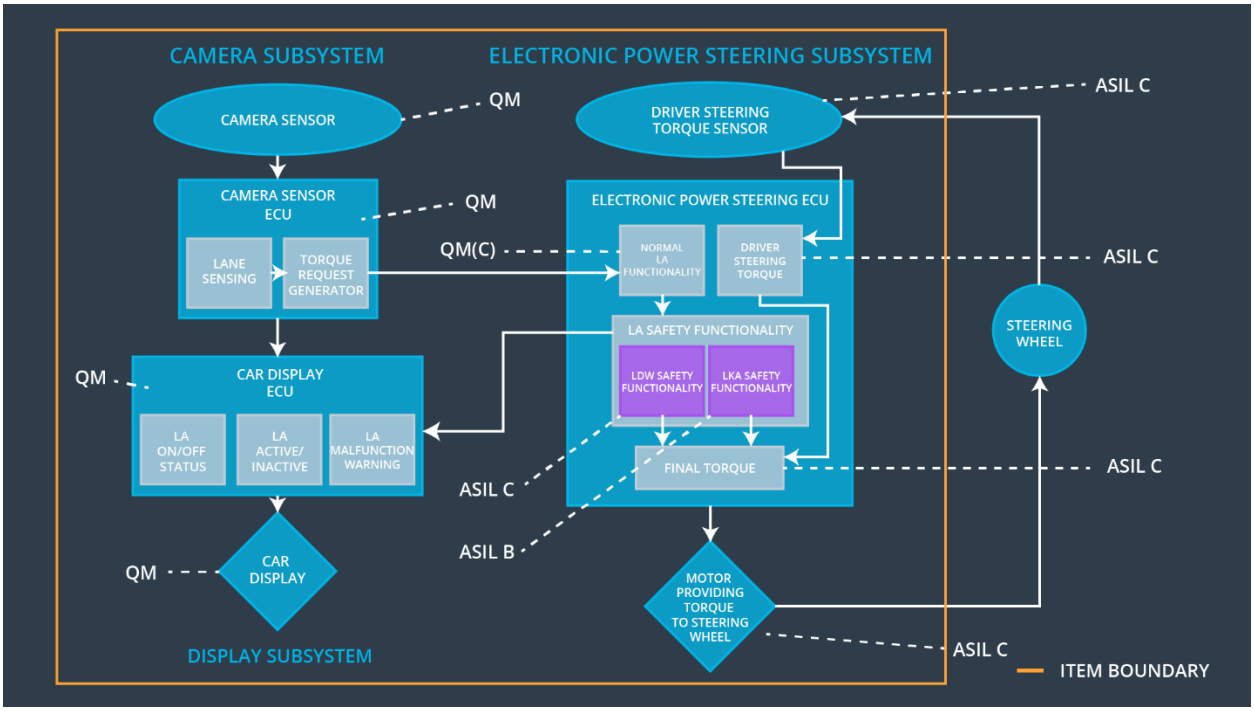

Figure 2. Refined System Architecture

The functional safety requirements for LKA and LDW are derived from ASIL B and C assigned safety goals. They are both allocated to the Power steering ECU. ASIL decomposition creates a single LA Safety Functionality module within the ECU in which two modules can assume the responsibility for meeting the functional safety requirements. These are assumed to be independent. If they were not independent, both would receive ASIL C ratings (the higher).

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	The lane keeping item shall	**X**		

Safety Requirement 01-02	ensure that the lane departure oscillating torque amplitude is below MAX_TORQUE_FREQUENCY.			
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 functionality	Violation of MAX_TORQUE_AMPLITUDE or MAX_TORQUE_FREQUENCY	Yes	Visual indication
WDC-02	Turn off functionality	Violation of MAX_DURATION	Yes	Visual indication