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
Sept 12 2017	0.1	RE	First Draft
Sept 13 2017	1.0	RE	INITIAL RELEASE

Table of Contents

Purpose of the Functional Safety Concept

A functional safety concept generates functional safety requirements from the general functional safety goals. These requirements are allocated to subsystems and parts of the system. The system architecture may require modification to meet the functional safety requirements. Each of the requirements has attributes relating to the ASIL level, the fault tolerant time interval and the safe state of the system. Verification and validation of the requirements are discussed. The functional safety concept reviews general functionality of an item but does not include the technical implementation of the design.

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 kepping 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.
Safety_Goal_03	The lane keeping assistance shall use self-diagnostics and track a confidence score in the lane measurement and position calculation. The system shall deactivate and warn the driver if the confidence score is too low.
Safety_Goal_04	The lane keep assistance shall deactivate if lane markings are not detected (due to adverse weather or other sensor obstruction).

Preliminary Architecture

The overall preliminary architecture of the system is provided in Figure 1.

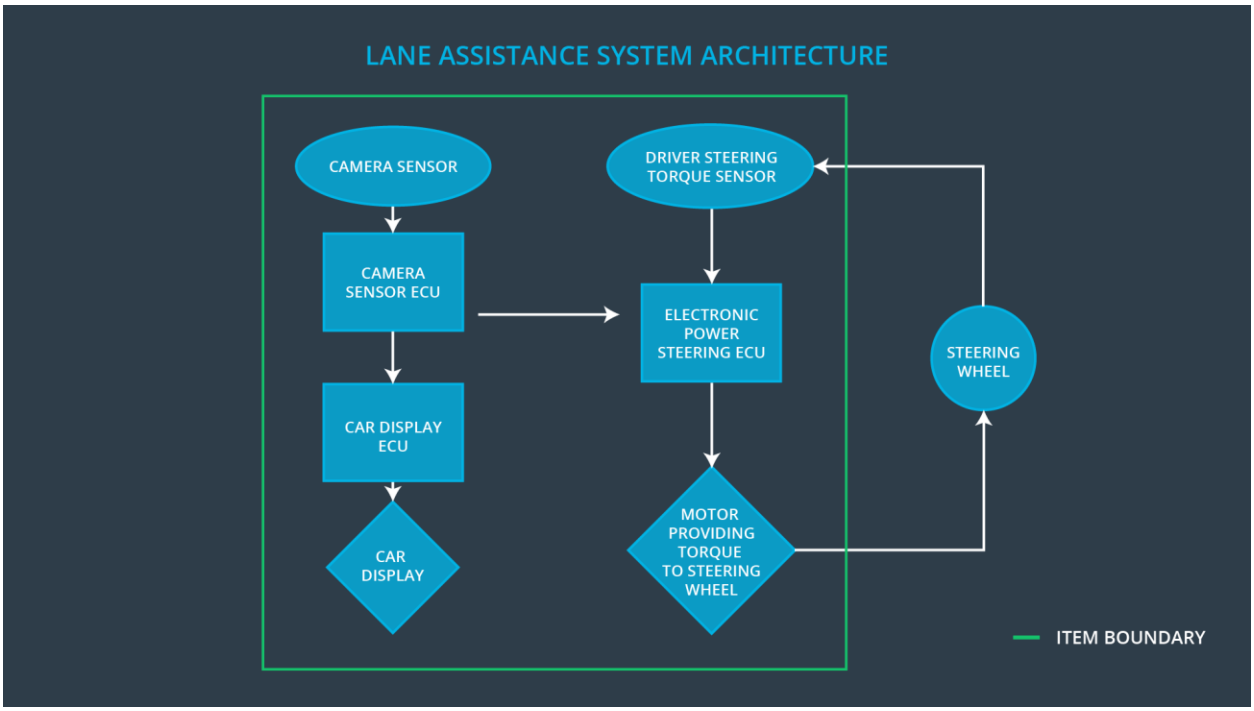

Figure 1: Preliminary architecture

Description of architecture elements

Element	Description
Camera Sensor	Physical sensor responsible for detecting lane lines
Camera Sensor ECU	Electronics hardware and processor or micro-controller responsible for interpreting camera data, identifying lane markings, determining vehicle position and issuing torque requests to the electronic power steering ECU
Car Display	Vehicle dashboard lights or display / screen unit providing status feedback to the driver of vehicle systems.
Car Display ECU	Electronics hardware responsible for interpreting input from other systems and controlling the lights or display unit.
Driver Steering Torque Sensor	Physical sensor such as an encoder or strain gauge capable of measuring steering torque input on the steering wheel from the driver.
Electronic Power Steering ECU	Electronics hardware responsible for accepting torque commands from other systems, monitoring the driver torque input and actuating the vehicle steering motor.

Motor	The motor which applies torque to the steering column, accepts voltage / current control from the 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 function applies an oscillating torque with very high torque amplitude (above limit)	Driver loses control of the vehicle. Collision with other vehicle or obstacle.
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	The lane departure warning function applies an oscillating torque with very high torque frequency (above limit)	Driver loses control of the vehicle. Collision with other vehicle or obstacle.
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 function is not limited in time duration which leads to misuse as an autonomous driving function.	LKA hardware and function is not adequate for autonomous driving. Collision with other vehicle or obstacle.
Malfunction_04	Lane Keeping Assistance (LKA)	The lane keeping assistance function	The vehicle is steered

	function identifies lane markings, determines vehicle position and issues torque requests to the power steering ECU	wrongly identifies lane markings	in an incorrect direction, resulting in a collision with other vehicle or obstacle
Malfunction_05	Lane Keeping Assistance (LKA) function identifies lane markings, determines vehicle position and issues torque requests to the power steering ECU	The lane keeping assistance camera sensor does not detect lane markings due to adverse weather obstructing the markings	The system does not actuate the steering wheel to stay in the lane.

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	turn off functionality
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	turn off functionality

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety	Driver testing is used to determine	Software testing is used to command a torque larger than Max_Torque_

Requirement 01-01	whether the Max_Torque_Amplitude value is controllable for most drivers	Amplitude, precision timing is used to ensure the system outputs zero torque within 50ms. A precision torque sensor instrument is used to verify that the Max_Torque_Amplitude setting is the value measured at the wheel.
Functional Safety Requirement 01-02	Driver testing is used to determine whether the Max_Torque_Frequency value is controllable for most drivers	Software testing is used to command a frequency larger than Max_Torque_ Frequency, precision timing is used to ensure the system outputs zero torque within 50ms. A precision frequency sensor instrument, such as an accelerometer is used to verify that the Max_Torque_Frequency setting is the value measured at the wheel.

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	turn off functionality

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	Driver testing is used to determine if applying assistance torque for only max_duration dissuades drivers from using the LKA as an autonomous function and keeping their hands off the wheel	Timing is used to verify that the lane keeping assistance function is turned off after max_duration.

Refinement of the System Architecture

Based on the functional safety concept and requirements, the refined system architecture is presented in Figure 2. Note that the Camera Sensor ECU is mistakenly labelled as a Car Display ECU.

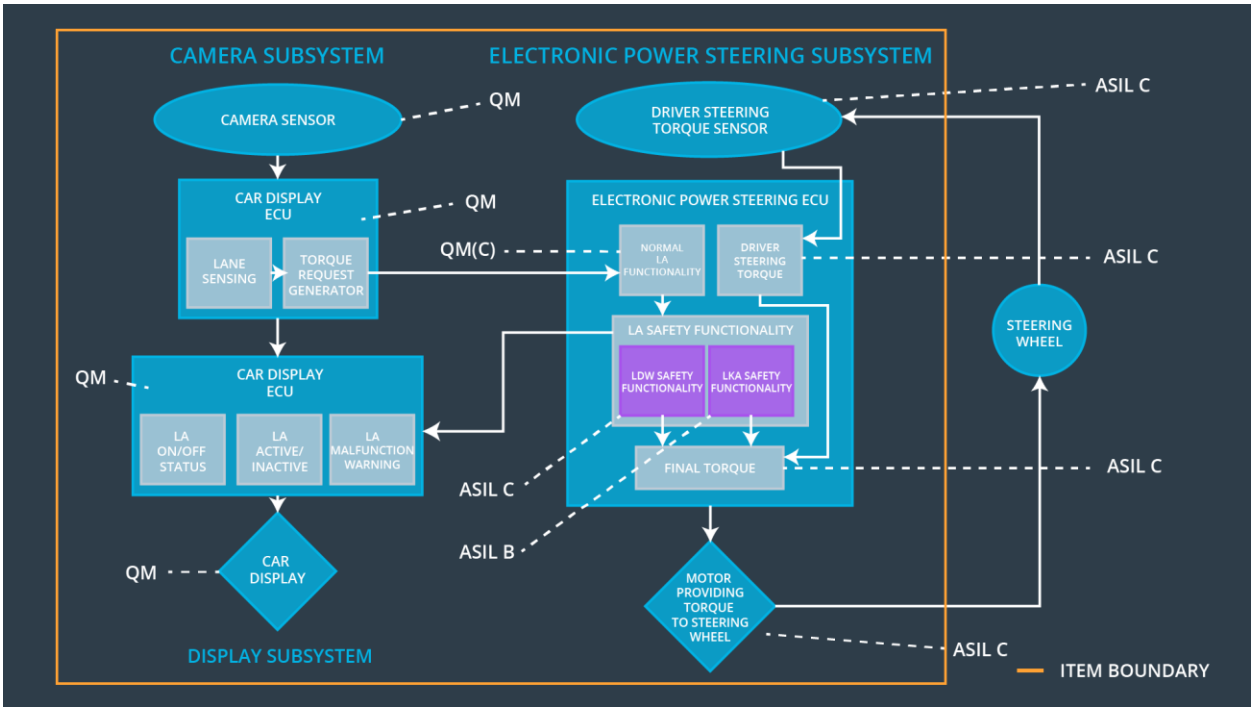

Figure 2: Refined System Architecture with ASIL labels

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	**NA**	**NA**
Functional Safety Requirement 01-02	Driver testing is used to determine whether the Max_Torque_Frequency value is	**X**	**NA**	**NA**

	controllable for most drivers			
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	**NA**	**NA**

Warning and Degradation Concept

ID	**Degradation Mode**	**Trigger for Degradation Mode**	**Safe State invoked?**	**Driver Warning**
WDC-01	turn off the functionality	Malfunction_01/ 02	yes	Car display
WDC-02	turn off the functionality	Malfunction_03	yes	Car display