Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Version 1.0, Released on 2017-08-18

Document history

Date	Version	Editor	Description
Aug 18, 2017	1.0	Jian Liang Linn	Initial Draft

Table of Contents

Purpose of the Functional Safety Concept

The purpose of this document is to identify the new system level requirement and specify these requirements to high level system diagrams for the Lane Assistance Functional Safety Project and to plan for the potential malfunctions of the system defined by ISO 26262 standard.

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 (LDW) system shall be limited
Safety_Goal_02	The Lane Keeping Assistance (LKA) system shall be time limited and the additional steering torque shall end after the time limit
Safety_Goal_03	The Camera Sensor ECU shall check malfunction warning status before sending torque request to the Lane Departure Warning (LDW) system
Safety_Goal_04	The Lane Keeping Assistance (LKA) system shall deactivate when the Camera Sensor ECU stops detecting the lane and shall notify the driver that LKA function is deactivated

Preliminary Architecture

The architecture of the system is shown in figure 1.

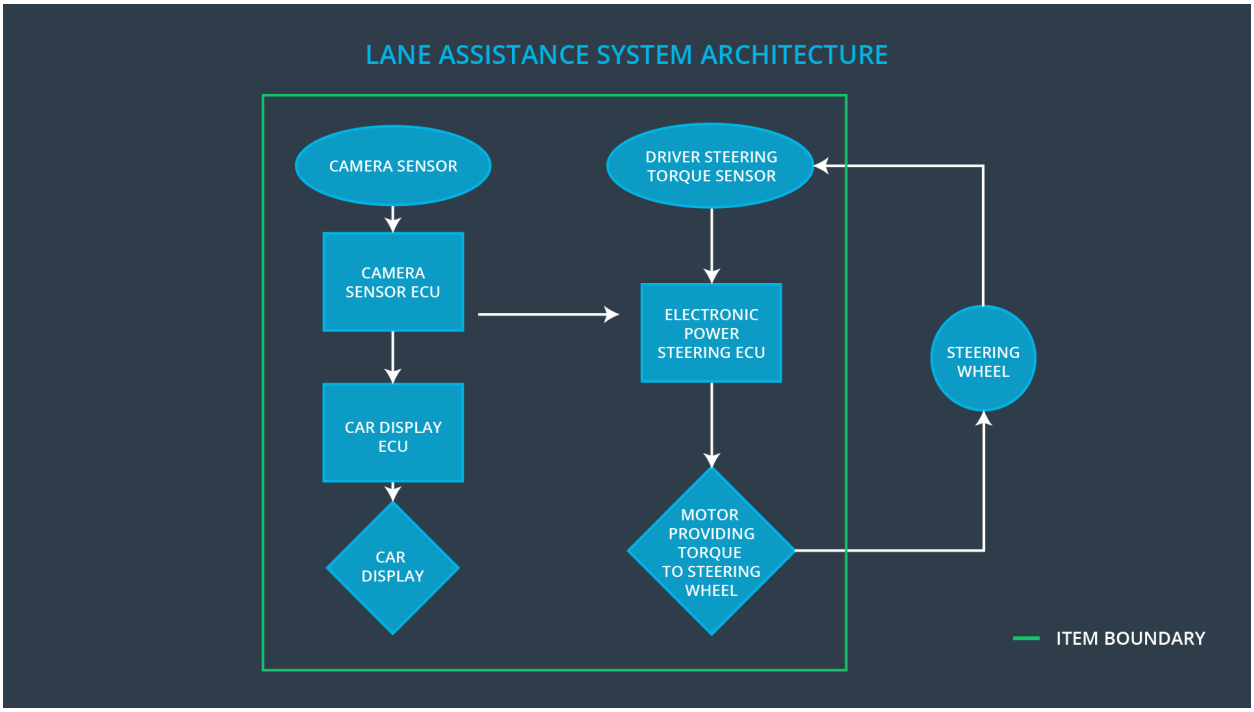

figure 1: Lane Assistance System Architecture

Description of architecture elements

Element	Description
Camera Sensor	Sensor for capturing the videos of road conditions and lane lines
Camera Sensor ECU	Detecting the lane lines and determining when the vehicle leaves the lane
Car Display	Display for warning and activation/deactivation of LDW and LKA functions
Car Display ECU	Displaying the warning of lane departure, LDW and LKA activation/deactivation on Car Display
Driver Steering Torque Sensor	Sensor for measuring how much steering torque the driver is applying to the steering wheel
Electronic Power Steering ECU	Measuring the torque provided by the driver and adding appropriate torque based on LKA request and vibrates the steering wheel with LDW warning when the driver goes out of lane by mistake
Motor	Applying requested torque t the steering by EPS ECU

	for either LDW or LKA functions.

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: Torque Amplitude is too much	The LDW function applies an very high torque amplitude to oscillate torque
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE: Torque frequency is too much	The LDW function apples very high torque frequency to oscillate torque
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	NO: LKA function always activated	The LKA function has no limitation in times for activation which leads to misuses
Malfunction _04	Lane Departure Warning (LDW) function shall apply	WRONG: LDW function unexpectedly activated	The LDW function unexpectedly activates to oscillate

	an oscillating steering torque to provide the driver with haptic feedback		the steering wheel
Malfunction_05	Lane Keeping Assistance (LKA) function shall apply the steering toque when it is active in order to stay in the lane	WRONG: the camera sensor detection is wrong	The LKA function is not able to detect 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 LKA function shall ensure that the lane departure oscillating torque amplitude is below MAX_TORQUE_AMPLITUDE	C	50 ms	Set vibration torque amplitude to zero
Functional Safety Requirement 01-02	The LKA function shall ensure that the lane departure oscillating torque frequency is below MAX_TORQUE_FREQUENCY	C	50 ms	Set vibration torque frequency 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	Validate MAX_TORQUE_AMPLITUDE is high enough to be detected by the driver while low enough not to cause loss of steering	Verify that the system really turn off if the lane departure warning exceeds MAX_TORQUE_AMPLITUDE
Functional Safety	Validate MAX_TORQUE_FREQUENCY is high enough to be detected by the	Verify that the system really turn off if the lane departure warning exceeds

Requirement 01-02	driver while low enough not to cause loss of steering	MAX_TORQUE_FREQUENCY

Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The EPS ECU shall ensure that the lane keeping assistance torque is applied for only MAX_DURATION	B	500 ms	Set lane keeping assistance torque to zero
Functional Safety Requirement 02-02	The EPS ECU shall ensure that the lane keeping assistance torque is set to zero when the Camera Sensor ECU stops detecting the lane and shall send the status (off) to the Car Display	B	500 ms	Set the lane keeping assistance torque to 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	Validate the MAX_DURATION really does persuade the drive not to take their hands of off the steering wheel	Verify that the system turns off after exceeding the MAX_DURATION
Functional Safety Requirement 02-02	Validate Camera Sensor ECU does not generate torque requests when the lane detection is lost	Verify that the system turns off when the camera sensor ECU loses the lane detection

Refinement of the System Architecture

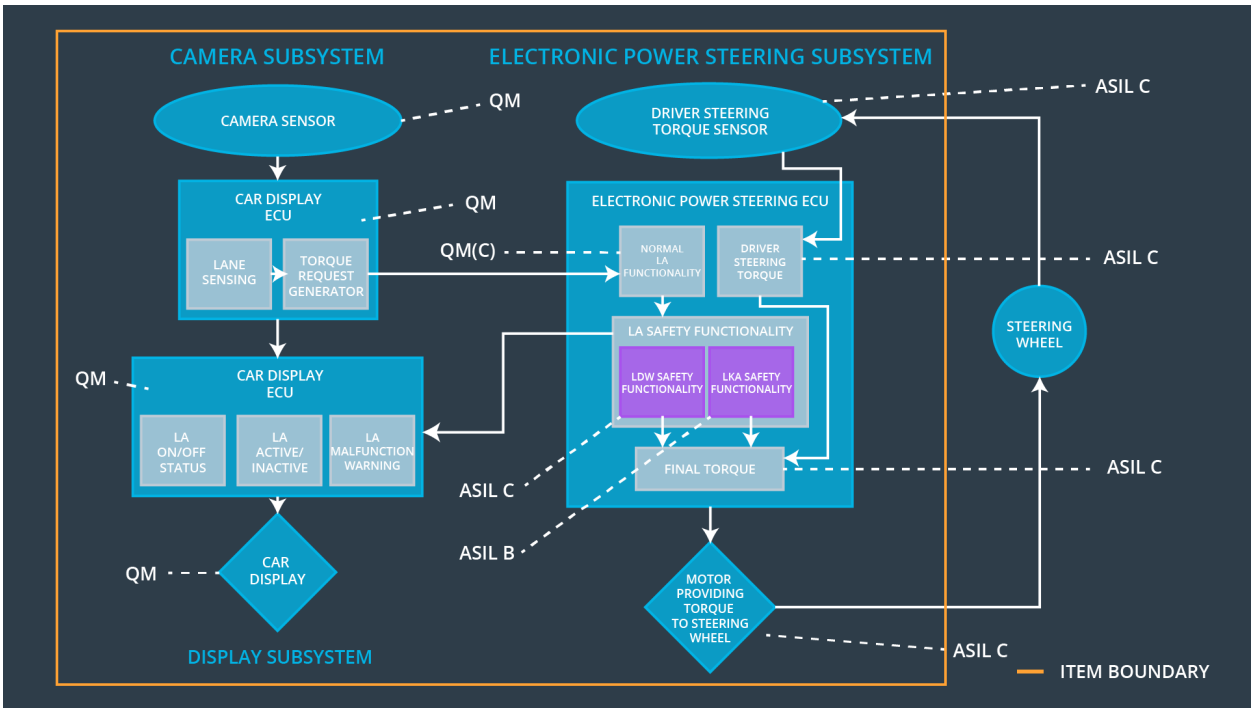

figure 2: refined system architecture with ASIL level assigned

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 LKA function shall ensure that the lane departure oscillating torque amplitude is below MAX_TORQUE_AMPLITUDE	**x**		
Functional Safety Requirement	The LKA function shall ensure that the lane departure oscillating	**x**		

01-02	torque frequency is below MAX_TORQUE_FREQUENCY			
Functional Safety Requirement 02-01	The EPS ECU shall ensure that the lane keeping assistance torque is applied for only MAX_DURATION	**x**		
Functional Safety Requirement 02-02	The EPS ECU shall ensure that the lane keeping assistance torque is set to zero when the Camera Sensor ECU stops detecting the lane and shall send the status (off) to the Car Display	**x**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW function	Malfunction_01, Malfunction_02	LDW torque shall be set to zero	Lane Assistance function inactive and Malfunction warning will be set and displayed in Car Display ECU and Car Display respectively
WDC-02	Turn off LKA function	Malfunction_03, Malfunction_05	LKA torque shall be set to zero	Lane Assist function inactive and Malfunction warning will be set and displayed in Car Display ECU and Car Display respectively