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
18 Mar 2018	1.0	Ong Whee Cheng	Initial version
19 Mar 2018	1.1	Ong Whee Cheng	Updated the safe state of Functional Safety Requirements after review

Table of Contents

Purpose of the Functional Safety Concept

Functional Safety Concept is a high level approach in the concept phase that looks at the general functionality of the item without going into the technical details. It identifies new functional safety requirements and allocates these requirements to the relevant parts of the system architecture.

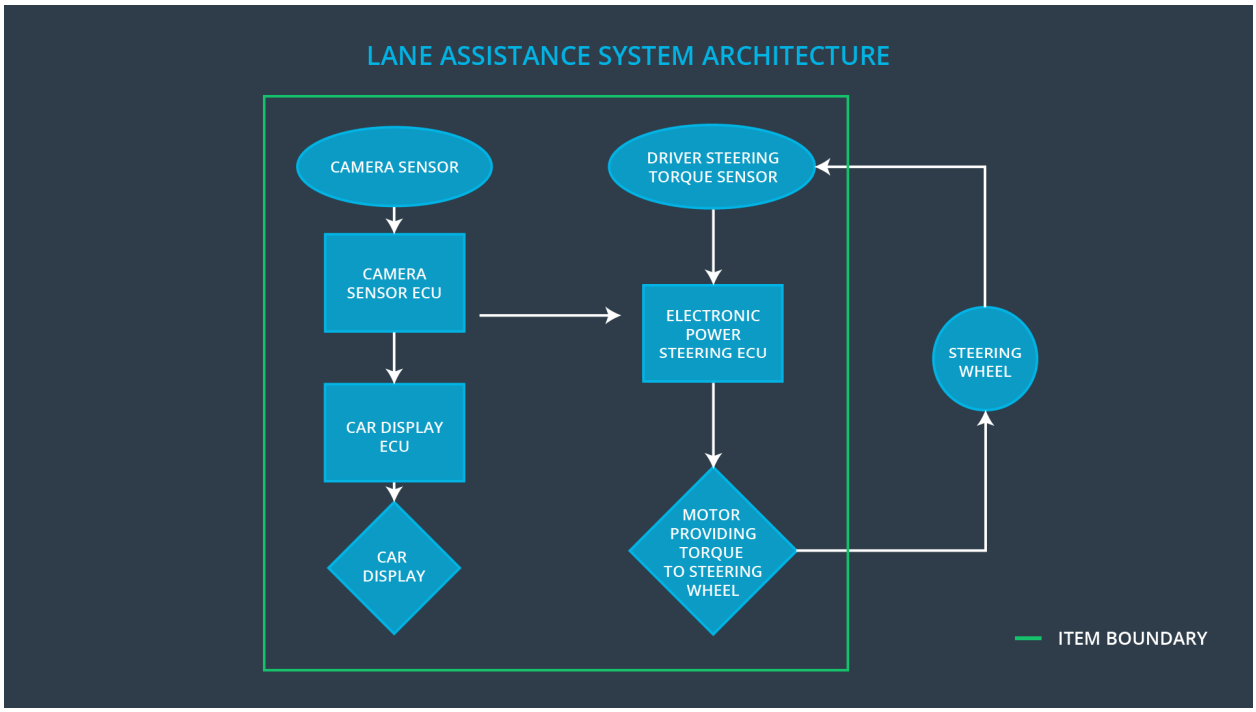
Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscillating steering torque from the Lane Departure Warning (LDW) function shall be limited
Safety_Goal_02	The Lane Keeping Assistance (LKA) function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver cannot misuse the system for autonomous driving
Safety_Goal_03	The LKA function shall apply a lower torque when the crosswind is in the same direction as the applied torque
Safety_Goal_04	The LKA function shall be deactivated if the camera sensor is unable to detect lanes correctly

Preliminary Architecture

The preliminary architecture of the Lane Assistance item is shown below:



Description of architecture elements

Element	Description
Camera Sensor	Provides camera images to the Camera Sensor ECU
Camera Sensor ECU	Detects lane line positions from camera images and generates a torque request to the Electronic Power Steering ECU if it determines the vehicle is departing from lane
Car Display	Provides visual feedback to the driver: • ACTIVE/INACTIVE status of Lane Departure Warning function • ON/OFF status of Lane Keeping Assistance function
Car Display ECU	Processes inputs from Camera Sensor ECU and generates visual signals to Car Display
Driver Steering Torque Sensor	Senses the current steering torque applied to the steering wheel
Electronic Power Steering ECU	Processes inputs from Camera Sensor ECU and Driver Steering Torque Sensor and determines the final steering torque to apply to the steering wheel motor

Element	Description
Motor	Applies the final steering torque from Electronic Power Steering ECU to the steering wheel

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 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	MORE	The LDW 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 LKA function is not limited in time duration which leads to misuse as an autonomous driving function
Malfunction_04	Lane Keeping Assistance (LKA) function shall apply	MORE	The vehicle over-steers if the crosswind is in the

Malfunction ID	Main Function of the Item Related to Safety Goal Violations	Guidewords (NO, WRONG, EARLY, LATE, MORE, LESS)	Resulting Malfunction
	the steering torque when active in order to stay in ego lane		same direction as the applied torque
Malfunction_05	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	NO	Camera sensor is unable to find lane lines due to snow

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	Set oscillating torque amplitude to 0
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C		Set oscillating torque frequency to 0

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	Test how drivers react to different torque amplitudes to prove that an appropriate value was chosen	Verify LDW function is deactivated within 50ms if torque amplitude exceeds Max_Torque_Amplitude

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement 01-02	Test how drivers react to different torque frequencies to prove that an appropriate value was chosen	Verify LDW function is deactivated within 50ms if torque frequency exceeds Max_Torque_Frequency

Lane Keeping Assistance (LKA) Requirements:

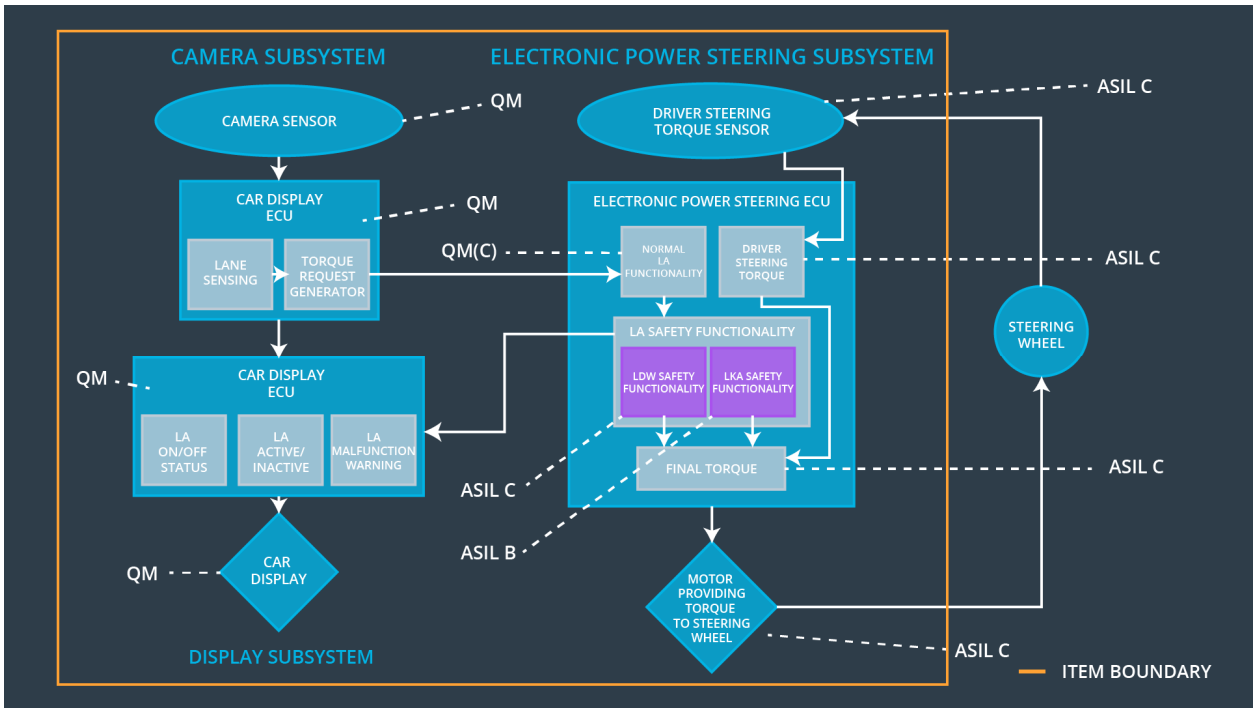
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500ms	Set LKA torque to 0
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that lane keeping assistance torque subtracts the effects of crosswind from the additional steering torque, i.e. Torque_Additional - Torque_Crosswind, if the crosswind is in the same direction as the applied steering torque	B	100ms	Set LKA torque to 0
Functional Safety Requirement 02-03	The electronic power steering ECU shall ensure that lane keeping assistance torque is 0 if Lane_Detected is false from the camera sensor ECU	A	50ms	Set LKA torque to 0

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	Test and validate that the Max_Duration chosen really did dissuade drivers from taking their hands off the wheel	Verify LKA function is deactivated within 500ms if LKA torque exceeds Max_Duration

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement 02-02	Test and validate that the final steering torque is the subtraction of the effects of crosswind from the additional steering torque, i.e. Torque_Additional – Torque_Crosswind, if the crosswind is in the same direction as the applied steering torque	Verify LKA function is deactivated within 100ms if LKA torque is greater than Torque_Additional – Torque_Crosswind
Functional Safety Requirement 02-03	Test and validate that Lane_Detected is false if lane lines cannot be detected	Verify LKA function is deactivated within 50ms if Lane_Detected is false

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 amplitude is below Max_Torque_Amplitude	X		
Functional Safety Requirement 01-02	The lane keeping item 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		
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that lane keeping assistance torque subtracts the effects of crosswind from the additional steering torque, i.e. Torque_Additional - Torque_Crosswind, if the crosswind is in the same direction as the applied steering torque	X		
Functional Safety Requirement 02-03	The electronic power steering ECU shall ensure that lane keeping assistance torque is 0 if Lane_Detected is false from the camera sensor ECU	X		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Lane Assistance is turned off	Malfunction_01	Yes	Lane Assistance Malfunction Warning on Car Display
WDC-02	Lane Assistance is turned off	Malfunction_02	Yes	Lane Assistance Malfunction Warning on Car Display
WDC-03	Lane Assistance is turned off	Malfunction_03	Yes	Lane Assistance Malfunction Warning on Car Display
WDC-04	Lane Assistance is turned off	Malfunction_04	Yes	Lane Assistance Malfunction Warning on Car Display
WDC-05	Lane Assistance is turned off	Malfunction_05	Yes	Lane Assistance Malfunction Warning on Car Display