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
12/30/2017	1.0	Me	First draft

Table of Contents

Purpose of the Functional Safety Concept

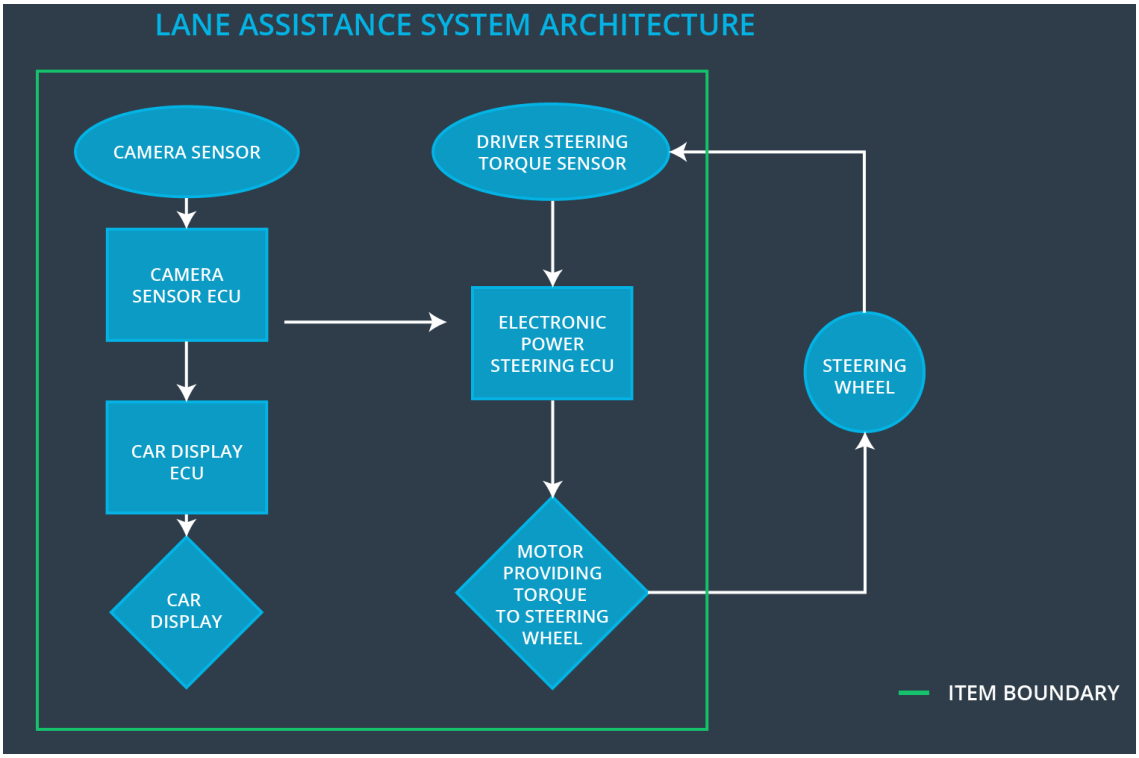
The Functional Safety Concept for the Lane Assistance (LA) item identifies the functional safety requirements for the LA item based on the previously identified safety goals and then allocates the requirements to the system architecture.

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 time interval so that the driver cannot misuse the system for autonomous driving

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Collects images of the external environment
Camera Sensor ECU	Processes the images and determines position of vehicle with respect to the lane. Identifies lane departure
Car Display	Notifies driver of current status of Lane Assistance feature
Car Display ECU	Backend for the Car Display; processes status from other subsystems and sends to Display
Driver Steering Torque Sensor	Measures the torque applied to the steering wheel by the driver
Electronic Power Steering ECU	Calculates the amount of torque to apply to the steering wheel given the current conditions
Motor	Applies the calculated torque 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 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	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

Lane Departure Warning (LDW) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Torque applied by the Lane Assistance item is zero
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	Torque applied by the Lane Assistance item is 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	Using simulations first and then with actual drivers, demonstrate that the amplitude of the LDW torque results in vehicle controllability and driver comfort/trust	Using analysis and testing methods, show that the LDW torque amplitude is set to 0 within 50ms of exceeding Max_Torque_Amplitude
Functional Safety Requirement 01-02	Using simulations first and then with actual drivers, demonstrate that the frequency of the LDW torque results in vehicle controllability and driver comfort/trust	Using analysis and testing methods, show that the LDW torque amplitude is set to 0 within 50ms of exceeding Max_Torque_Frequency

Lane Keeping Assistance (LKA) Requirements:

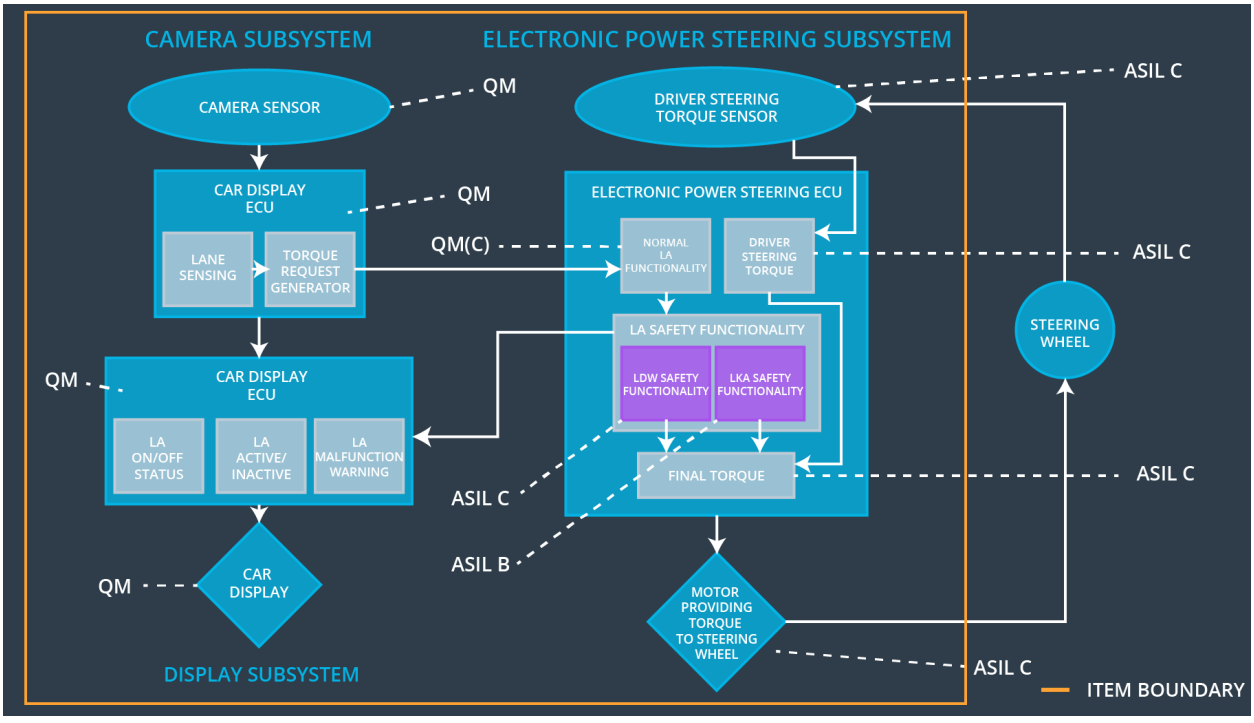
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional	The electronic power steering ECU shall	B	500ms	Torque applied

Safety Requirement 02-01	ensure that the lane keeping assistance torque is applied for only Max_Duration			by the Lane Assistance item is 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	Demonstrate with actual drivers that they understand that they should not take their hands off the wheel.	Using analysis and testing methods, show that the LKA torque is set to 0 if the Lane Assistance is active for over 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 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		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off Lane Departure Warning functionality	Malfunction_01 Malfunction_02	Yes	Lane Assist malfunction warning provided by Car Display
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03	Yes	Lane Assist malfunction warning provided by Car Display