Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 3.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
2018-03-13	1.0	Abhishek Mantha	Document initialization
2018-03-13	2.0	Abhishek Mantha	Revising for Final Submission
2018-03-14	3.0	Abhishek Mantha	Final Submission

Table of Contents

Purpose of the Functional Safety Concept

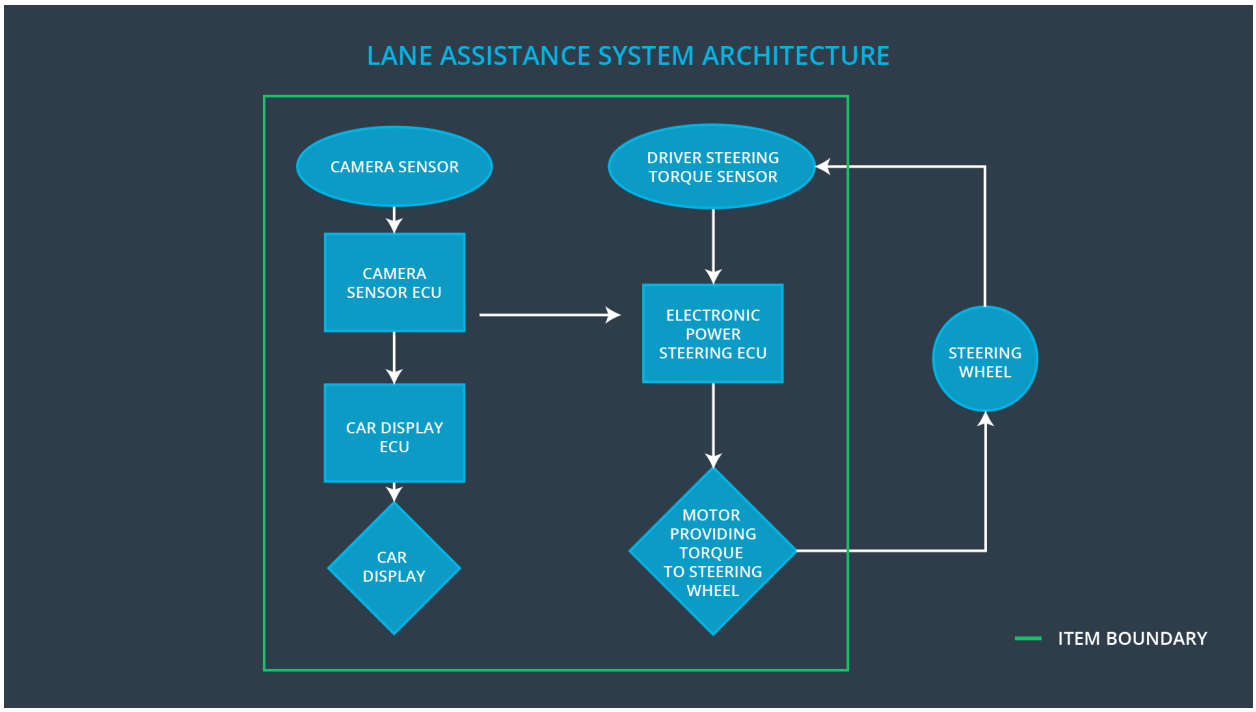
The functional safety concept allocates identified functional safety requirements to the relevant parts of the system diagram. Allocation means defining which part of the system architecture will implement each requirement. Functional safety requirements are specified with attributes such as: ASIL level; fault tolerant time interval, which measure how quickly a system needs to react to a hazardous situation; safe state, which discusses what a system looks like after it has avoided an accident. Finally, the functional safety concepts address verification and validation processes to prove the system actually meets requirements.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	Oscillating steering torque from LDW function shall be limited.
Safety_Goal_02	LKA function shall be time limited so that driver cannot misuse the system for autonomous driving.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	The Camera Sensor reads in images from road.
Camera Sensor ECU	The Camera Sensor ECU identifies when the vehicle has accidentally departed its lane, and sends the appropriate messages to the Car Display ECU and the Electronic Power Steering ECU.
Car Display	The Car Display displays notifications on driver

	dashboard.
Car Display ECU	The Car Display ECU sends messages to be displayed by the Car Display, triggered by incoming input from the Camera Sensor ECU.
Driver Steering Torque Sensor	The Driving Steering Torque Sensor records current steering wheel torque.
Electronic Power Steering ECU	The Electronic Power Steering ECU combines data from Camera Sensor ECU and Driver Steering Torque Sensor to determine amount of oscillating torque to apply, depending on amount steering wheel is already turned and if unsafe lane departure has occurred. The Electronic Power Steering ECU sends a signal to motor controlling steering wheel torque to apply physical force.
Motor	The Motor applies the torque to steering wheel specified by the Electronic 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 LDW warning is giving **MORE** torque than what is safe.	The LDW function applies an oscillating torque with very high torque amplitude (above limit).
Malfunction_02	Lane Departure Warning (LDW)	The LDW warning is giving **MORE** torque	The LDW function applies an oscillating

	function shall apply an oscillating steering torque to provide the driver a haptic feedback	than what is safe.	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	The LKA function has **NO** time limit.	The LKA 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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 ms	LDW will 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	50 ms	LDW will set oscillating torque amplitude 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	**Criteria**: Test how drivers react to different torque amplitudes to prove selection of an appropriate Max_Torque_Amplitude **Method**: Live driving simulations	**Criteria**: When torque amplitude crosses Max_Torque_Amplitude, lane assistance output is set to 0 within 50 ms fault tolerant time interval **Method**: software test inserting fault into system to observe results
Functional Safety Requirement	**Criteria**: Test how drivers react to different torque frequencies to prove selection of an appropriate	**Criteria**: When torque frequency crosses Max_Torque_Frequency, lane assistance output is set to 0 within 50

01-02	Max_Torque_Frequency **Method**: Live driving simulations	ms fault tolerant time interval **Method**: Software test

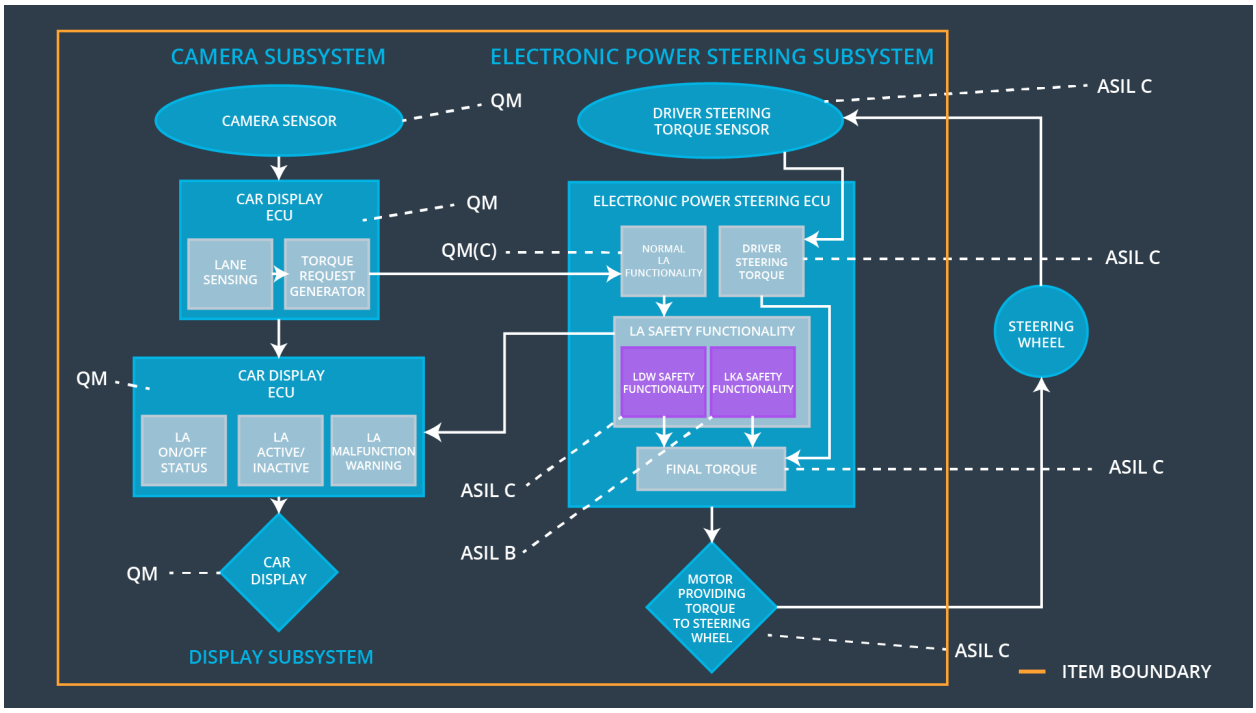
Lane Keeping Assistance (LKA) Requirements:

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	500 ms	LKA will set oscillating torque amplitude 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	**Criteria**: Test if drivers are dissuaded from taking hands off wheel based on selected Max_Duration value **Method**: Live driving simulations	**Criteria**: When max duration crosses Max_Duration, lane assistance output is set to 0 within 500 ms fault tolerant time interval **Method**: Software test

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	Electronic Power Steering ECU shall ensure that oscillating torque amplitude requested by LDW function is below Max_Torque_Amplitude.	**x**	**--**	**--**
Functional Safety Requirement 01-02	Electronic Power Steering ECU shall ensure that oscillating torque frequency requested by LDW function is below Max_Torque_Frequency.	**x**	**--**	**--**
Functional Safety Requirement	Electronic Power Steering ECU shall ensure that lane keeping assistance torque requested by	**x**	**--**	**--**

02-01	LKA function is applied for only Max_Duration.			

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	LDW disabled; torque request will be set to 0.	The LDW warning is giving **MORE** torque than what is safe.	Yes	Warning light appears on dashboard.
WDC-02	LKA disabled; torque request will be set to 0.	The LKA function has **NO** time limit.	Yes	Warning light appears on dashboard