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
4/29/2018	1.0	Yury Astashonok	First revision

Table of Contents

Purpose of the Functional Safety Concept

The purpose of the Functional Safety Concept is to identify functional safety requirement for the Lane Assistance item and allocate the requirements to the system architecture.

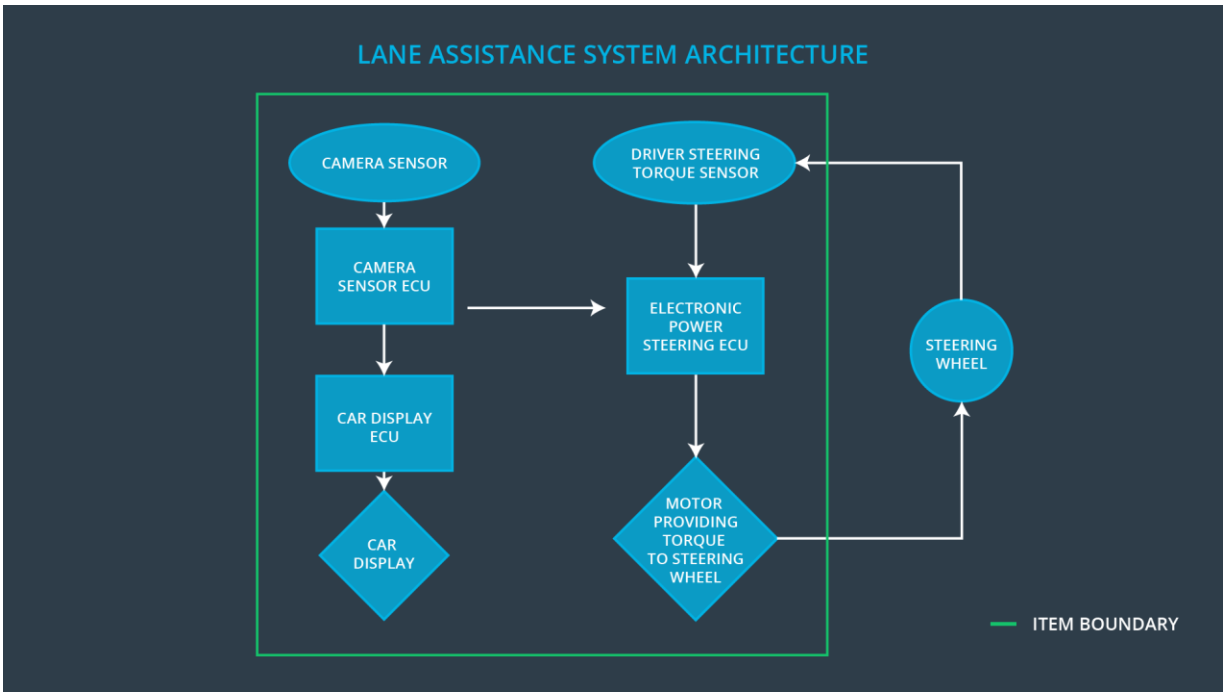
Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal

Safety_Goal_01	The oscillating steering torque from the lane departure warning function shall be limited.
Safety_Goal_02	The frequency of the oscillating feedback from the lane departure warning function shall be above a threshold.
Safety_Goal_03	The lane keeping assistance function shall apply steering torque only when activated so the driver doesn't lose control of the vehicle.
Safety_Goal_04	The lane keeping 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.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	The Camera Sensor reads in images from the road.
Camera Sensor ECU	The Camera Sensor ECU identifies when the vehicle is leaving the lane, and sends signals Electronic Power Steering ECU and Car Display ECU.
Car Display	The Car Display provides a visual feedback to the

	driver by turning on status lights.
Car Display ECU	The Car Display ECU sends a signal to the Car Display to turn on status lights.
Driver Steering Torque Sensor	The Driver Steering Torque Sensor detects the amount of torque applied by the driver to the steering wheel.
Electronic Power Steering ECU	The Electronic Power Steering ECU sends a signal to the Motor to apply extra steering torque.
Motor	The Motor provides a haptic feedback to the driver by adding extra 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	The oscillating steering torque from the lane departure warning function shall be limited.	MORE	The lane departure warning function applies an oscillating torque with very high torque amplitude (above limit)
Malfunction_02	The oscillating steering torque from the lane departure warning function shall be limited.	MORE	The lane departure warning function applies an oscillating torque with very high torque frequency (above limit)
Malfunction_03	The frequency of the	LESS	The lane departure

	oscillating feedback from the lane departure warning function shall be above a threshold.		warning function applies an oscillating torque with very low or no torque frequency (below limit).
Malfunction_04	The lane keeping assistance function shall apply steering torque only when activated so the driver doesn't lose control of the vehicle.	NO	The lane keeping assistance function applies steering torque when function is not activated.
Malfunction_05	The lane keeping 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.	NO	The lane keeping assistance function is not limited in time duration.

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	The Lane Assistance functionality is switched off.
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	The Lane Assistance functionality is switched off.

Functional Safety Requirement 01-03	The lane keeping item shall ensure that the lane departure oscillating torque frequency is above Min_Torque_Frequency.	B	50 ms	The Lane Assistance functionality is switched off.

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 driver reaction to different torque amplitudes.	Implement a software test suite to ensure the output torque amplitude does not exceed Max_Torque_Amplitude
Functional Safety Requirement 01-02	Test driver reaction to different torque frequencies.	Implement a software test suite to ensure the output torque frequency does not exceed Max_Torque_Frequency
Functional Safety Requirement 01-03	Test driver reaction to different torque amplitudes.	Implement a software test suite to ensure the output torque frequency does not fall below Min_Torque_Frequency

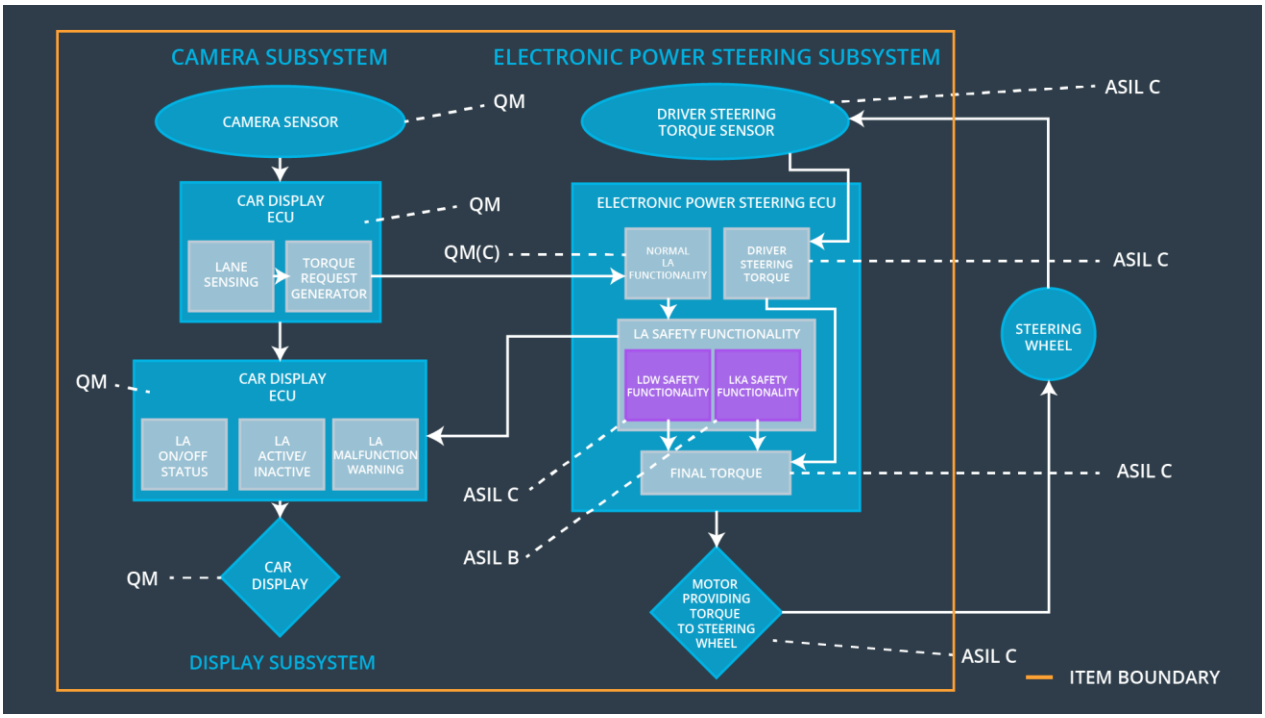
Lane Keeping Assistance (LKA) Requirements:

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 only when the function is activated.	C	50 ms	The Lane Assistance functionality is switched off.
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500 ms	The Lane Assistance functionality is switched off.

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 driver reaction to applied steering torque when the LKA system is not activated.	Implement a software test suite to ensure the output torque is not applied with LKA is off.
Functional Safety Requirement 02-02	Test driver reaction to steering torque applied for long durations.	Implement a software test suite to ensure the LKA does not output torque for longer than 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	The Electronic Power Steering	X		

Safety Requirement 01-01	ECU shall ensure that the oscillating torque amplitude requested by the LDW function is below Max_Torque_Amplitude.			
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 01-03	The lane keeping item shall ensure that the lane departure oscillating torque frequency is above Min_Torque_Frequency.	**X**		
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied only when the function is activated.	**X**		
Functional Safety Requirement 02-02	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 the functionality	LDW applies oscillating torque with amplitude above Max_Torque_Amplitude	Yes	Turn on the Lane Assistance Malfunction light on the dashboard.
WDC-02	Turn off the functionality	LDW applies oscillating torque with frequency above Max_Torque_Frequency	Yes	Turn on the Lane Assistance Malfunction light on the dashboard.
WDC-03	Turn off the functionality	LDW applies oscillating torque with frequency below Min_Torque_Frequency	Yes	Turn on the Lane Assistance Malfunction light on the dashboard.

WDC-04	Turn off the functionality	LKA applies torque when not activated	Yes	Turn on the Lane Assistance Malfunction light on the dashboard.
WDC-05	Turn off the functionality	LKA applies torque longer than Max_Duration	Yes	Turn on the Lane Assistance Malfunction light on the dashboard.