Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

Date	Version	Editor	Description
5/1/2019	1.0	Jiaxing Gao	First Commit

Table of Contents

Purpose of the Functional Safety Concept

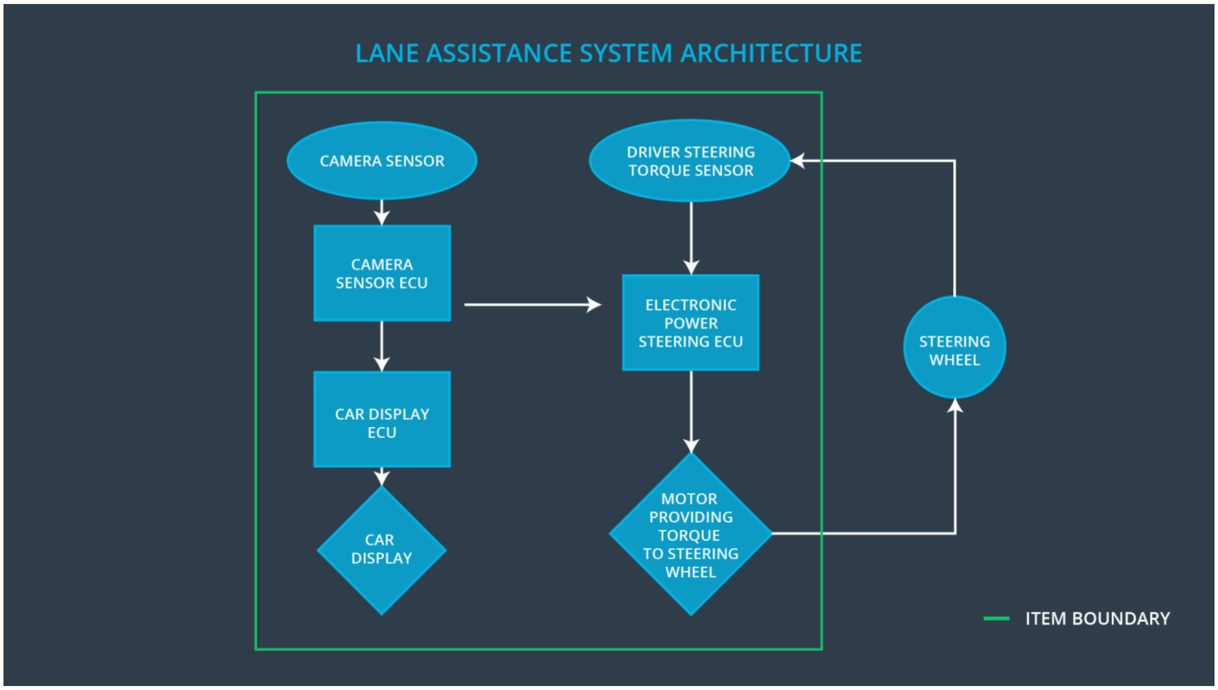
The Functional Safety Concept is a higher-level approach to define the general functionality of the item without going into deep technical detail, which should be considered in Technical Safety Concept. The goal is to identify safety requirements and then allocate these requirements to different parts of the item architecture. From the result of the functional safety concept, the technical safety requirements can be derived within a subsequent technical safety concept. Finally, to prove a system actually meets requirements, they have to be validated and verified.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	**Safety Goal**
Safety_Goal_01	The LDW shall has another indicator on the screen or other place to indicate its status, if it was not activated after driver turning it on, the LDW indicator should be red
Safety_Goal_02	The Lane Keeping Assistance function shall be time limited, and additional steering torque shall end after a given time interval so the driver cannot misuse the system for autonomous driving.
Safety_Goal_03	The oscillating steering torque from the Lane Departure Warning function shall be limited.
Safety_Goal_04	The Lane Keeping Assistance function shall be deactivated when the camera sensor stops working.

Preliminary Architecture


LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
CAMERA SENSOR ECU
CAR DISPLAY ECU
CAR DISPLAY
DRIVER STEERING TORQUE SENSOR
ELECTRONIC POWER STEERING ECU
MOTOR PROVIDING TORQUE TO STEERING WHEEL
STEERING WHEEL
ITEM BOUNDARY

Description of architecture elements

Element	Description
Camera Sensor	Capture RGB road image to send them to the Camera Sensor ECU
Camera Sensor ECU	Analyze input image to calculate the vehicle position relative to the road lanes
Car Display	Display warning to the driver and LDA status
Car Display ECU	Receive signal from other ECUs, like Camera Sensor ECU, and display information on the Car Display Screen as designed
Driver Steering Torque Sensor	Measure the torque applied from driver to the steering wheel
Electronic Power Steering ECU	Use the information received from the driver steering torque sensor and the torque requested by the LKA and LKW and request the necessary toque to be applied by the motor actuator
Motor	Receive the signal from EPS ECU and applied 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

[Instructions: Fill in the functional safety analysis table below.]

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
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
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 lead to misuse as an autonomous driving function
Malfunction_04	The Lane Keeping Assistance function shall be deactivated	WRONG	The Lane Keeping Assistance start acting randomly

	when the camera sensor stops working.		when the camera is not working
Malfunction_05	The LDW shall has another indicator on the screen or other place to indicate its status, if it was not activated after driver turning it on, the LDW indicator should be red	MORE	The LDW function didn’t have indication when the function didn’t activated after driver turned it on

Functional Safety Requirements

[Instructions: Fill in the functional safety requirements for the lane departure warning]

Lane Departure Warning (LDW) Requirements:

ID	**Functional Safety Requirement**	**ASIL**	**Fault Tolerant Time Interval**	**Safe State**
Functional Safety Requirement 01-01	The Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 ms	Vibration torque amplitude below Max_Torque_Amplitude.
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 ms	Vibration frequency is below Max_Torque_Frequency.
Functional Safety Requirement 01-03	There is another status in the system display on Car Display system to indicate the current status of LDW	QM	10 ms	Other indicator should be added

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 chosen is high enough to be detected by a driver while low enough not to cause loss of steering	Verify the system does turn off if the Lane Departure Warning exceeded Max_Torque_Amplitude.
Functional Safety Requirement 01-02	Validate Max_Torque_Frequency chosen is adequate to be detected by the driver and not cause the loss of steering.	Verify the system does turn off if the Lane Departure Warning exceeded Max_Torque_Frequency.
Functional Safety Requirement 01-03	Indicator of a ready LDW system should be added, LDW_Status, on Car Display system or other place for driver to notice	When the LDW system is ready LDW_Status does turn green when LDW system is ready

[Instructions: Fill in the functional safety requirements for the lane keeping assistance]

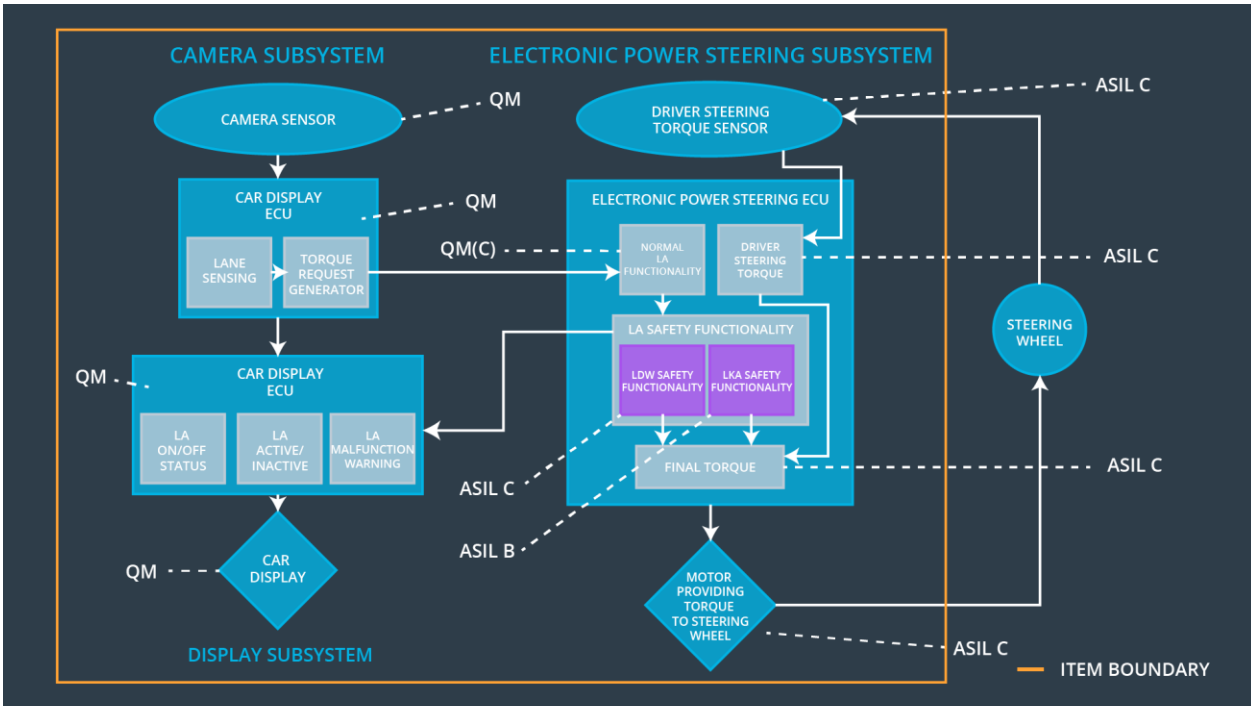
Lane Keeping Assistance (LKA) Requirements:

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 Max_Duration.	B	500 ms	Lane Keeping Assistance torque is zero.
Functional Safety Requirement 02-02	The Lane Keeping assistance shall be deactivated when the electronic power steering ECU detects the camera sensor is not working.	C	10 ms	Function is deactivated.

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 chosen not allow the driver to use the car as self-driving car.	Verify the system does deactivate if the Lane Keeping Assistance torque application exceeded Max_Duration.
Functional Safety Requirement 02-02	Validate the Lane Keeping assistance shall be deactivated when the camera sensor stop working.	Verify the system does deactivate the Lane Keeping Assistance if the camera sensor is not working.

Refinement of the System Architecture



Allocation of Functional Safety Requirements to Architecture Elements

[Instructions: Mark which element or elements are responsible for meeting the functional safety requirement. Hint: Only one ECU is responsible for meeting all of the requirements.]

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-01	The Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	**X**		
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	**X**		
Functional Safety Requirement 01-03	Indicator of a ready LDW system should be added, LDW_Status, on Car Display system or other place for driver to notice		**X**	**X**
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only Max_Duration.	**X**		
Functional Safety Requirement 02-02	The Lane Keeping assistance shall be deactivated when the electronic power steering ECU detects the camera sensor is not working.	**X**		

Warning and Degradation Concept

[Instructions: Fill in the 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, Malfunction_04 Malfunction_05	Yes	Lane Departure Warning Malfunction Warning on Car Display
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03	Yes	Lane Keeping Assistance Malfunction Warning on Car Display