Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
12/24/2018	1.0	melsobky	Initial version

Table of Contents

Purpose of the Functional Safety Concept

The functional safety concept is a high level that looks at the general functionality of the item without going into technical details to identify safety requirements and then allocate those requirements to different parts of the item architecture. From the result of the functional safety concept technical safety requirements can be derived. These requirements have to be verified and validated to prove that a system actually meets requirements.

Inputs to the Functional Safety Concept

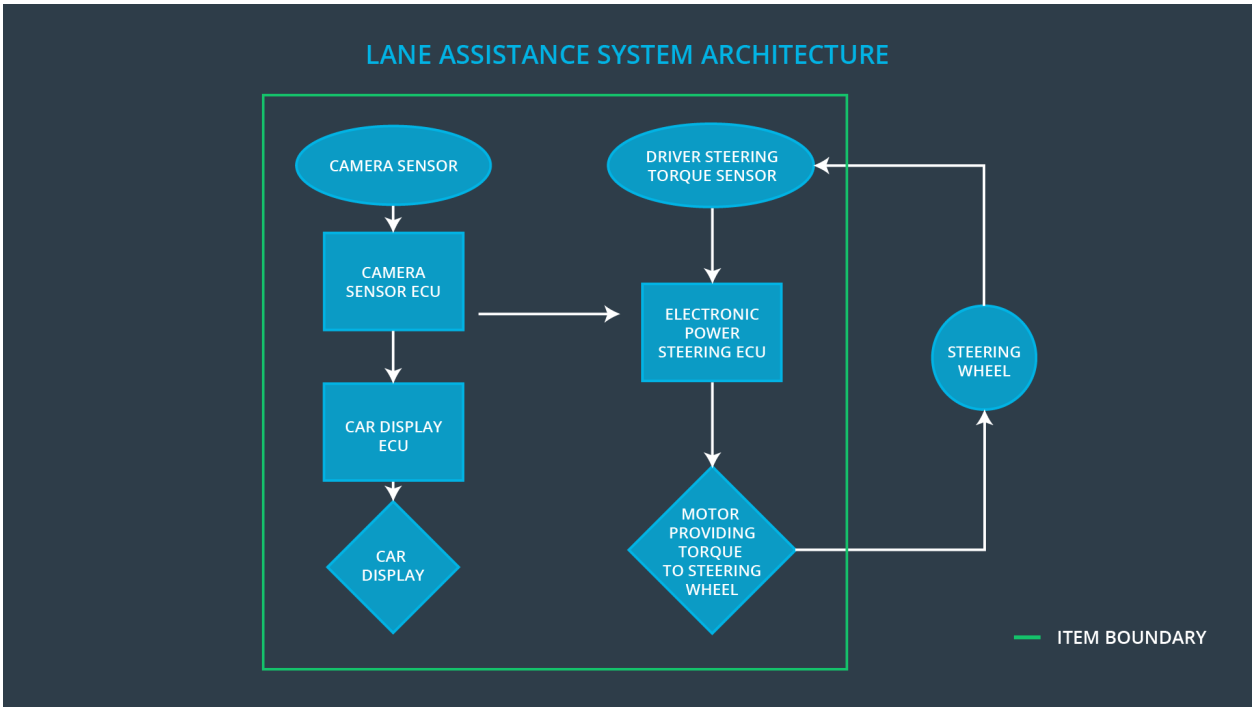
Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal

Safety_Goal_01	The oscillating steering torque from the lane departure warning function shall be limited
Safety_Goal_02	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
Safety_Goal_03	LKA function activation must be only triggered by the used and there must be multiple accessible ways to deactivate the function
Safety_Goal_04	The Oscillating steering torque from the LDW function shall be limited

Preliminary Architecture

The preliminary architecture for the lane assistance item is as bellow



Description of architecture elements

[Instructions: Provide a description for each of the item elements; what is each element's purpose in the lane assistance item?]

Element	Description
Camera Sensor	The camera sensor reads in images from the 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	Shows warning and indications to the driver
Car Display ECU	Drive the car display component to show LKA status and LDW warnings
Driver Steering Torque Sensor	Measure the torque applied by the driver to the steering wheel
Electronic Power Steering ECU	Uses the drivr requested torque and the torque requested by LKA and LDW to request the needed torque from the motor
Motor	Applies the requested torque by the EPS 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

[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 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 lane keeping item shall ensure that the lane departure oscillating torque *amplitude* is below Max_Torque_Amplitude	C	50 ms	Lane Assistant functionality 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	Lane Assistant functionality 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	Make sure that the selected Max_Torque_Amplitude is not too high that can cause loss for control or very low that it’s not detected by the driver	Verify that system turns off if LKA torque exceeds Max_Torque_Amplitude.
Functional Safety Requirement 01-02	Make sure that the selected Max_Torque_Frequency is not too high that can cause loss for control or very low that it’s not detected by the driver	Verify that system turns off if LKA frequency exceeds Max_Torque_Frequency.

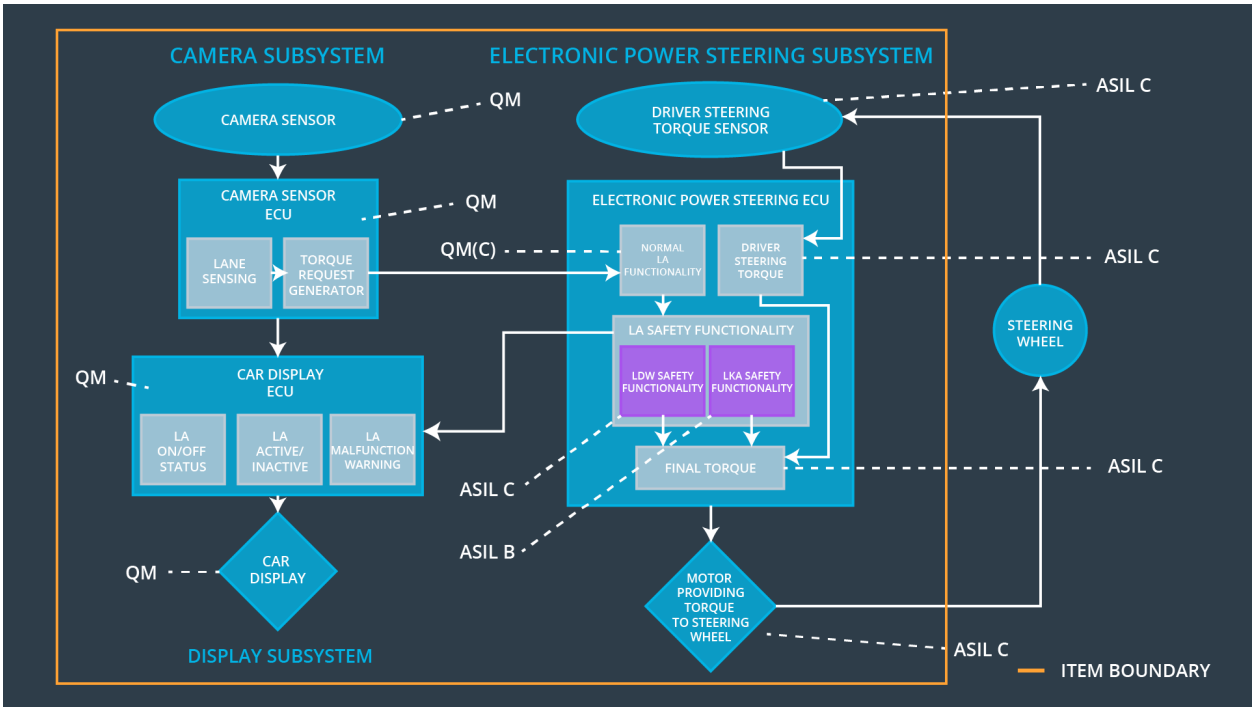
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500 ms	Lane Assistant functionality 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	Make sure that the selected Max_Duration really prevents drivers from taking their hands off the wheel.	Verify that system turns off if LKA time exceeds 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 electronic power steering ECU shall ensure that the lane departure oscillating torque *amplitude* is below Max_Torque_Amplitude	**X**		
Functional Safety Requirement 01-02	The electronic power steering ECU 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 LDW function	Malfunction_01, Malfunction_02	Yes	LDW malfunction warning on Dar Display
WDC-02	Turn off LKA function	Malfunction_03	Yes	LKA malfunction warning on Dar Display