Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [0.1]

Document history

Date	Version	Editor	Description
24.08.2017	0.1	Aneeq Mahmood	Functional safety description

Table of Contents

Purpose of the Functional Safety Concept

[Instructions: Answer what is the purpose of a functional safety concept?]

Functional safety concept (FSC) takes safety requirements arising from hazard analysis and risk assessment, and set goals within the system architecture to overcome the potential hazards and make the whole process safer. FSC incorporates changes at a higher level and does not deal with technical specifications for bringing about the required changes to the system architecture.

Inputs to the Functional Safety Concept

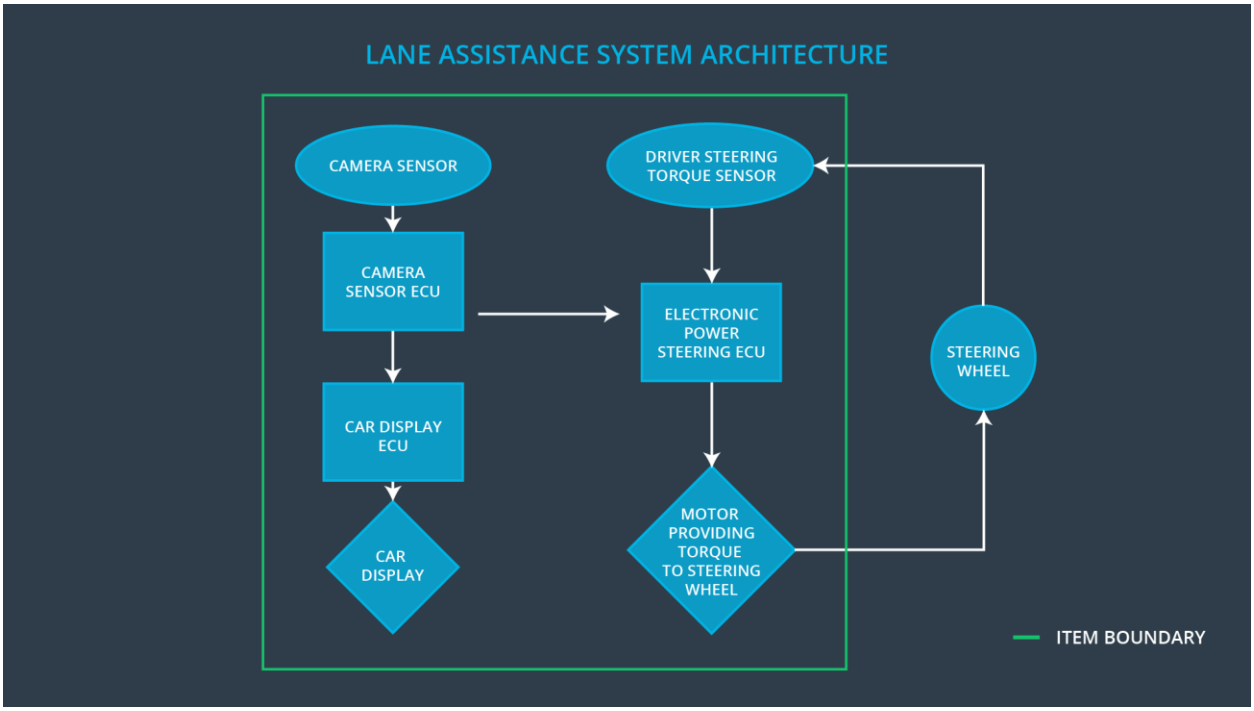
Safety goals from the Hazard Analysis and Risk Assessment

[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.
]

ID	Safety Goal
Safety_Goal_01	The oscillating steering from torque from the lane departure warning (LDW) function should be limited
Safety_Goal_01	The lane keeping assistance (LKA) function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver cannot misuse the system for autonomous driving

Preliminary Architecture

[Instructions: Provide a preliminary architecture for the lane assistance item. Hint: See Lesson 3: Item Definition]



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	Captures the road and sends the captured frames to the camera sensor ECU
Camera Sensor ECU	Using the information from the camera sensor, it determines the lane boundaries and notifies the car display system and power steering ECU if the car leaves the lane
Car Display ECU	Takes input form camera ECU and control the logic for activating or deactivating LEDs showing the status of LKA and LDW at car display
Car Display	Takes the input from car display ECU to turn the LEDS Off or On
Driver Steering Torque Sensor	Measures the torque coming from the driver
Electronic Power Steering (EPS) ECU	Takes input from camera ECU and current driver torque sensor to compute necessary torque for LKA, and assesses the torque amplitude and frequency for LKA
Motor	Takes its input from the EPS ECU and responsible for providing torque to the steering wheel and also

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 freqeuncy (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 LKA function is not limited in time duration which leads to misuse as an autonomous driving function

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 EPS ECU shall ensure that the oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Off
Functional Safety Requirement 01-02	The EPS ECU shall ensure that the oscillating torque amplitude is below Max_Torque_Frequency	C	50 ms	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	After fixing a limit on Max_Torque_Amplitude, test will be done to see how drivers react to different torque to prove that an appropriate value has been chosen	When the torque magnitude becomes greater than Max_Torque_Amplitude, the LKA system's output is set to zero within the 50 ms fault tolerant time interval
Functional Safety Requirement 01-02	After fixing a limit on Max_Torque_Frequency, test will be done to see how drivers react to different torque frequencies to prove that an appropriate value has been chosen	When the torque frequency becomes greater than Max_Torque_Frequency, the LKA system's output is set to zero within the 50 ms fault tolerant time interval

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

Lane Keeping Assistance (LKA) Requirements:

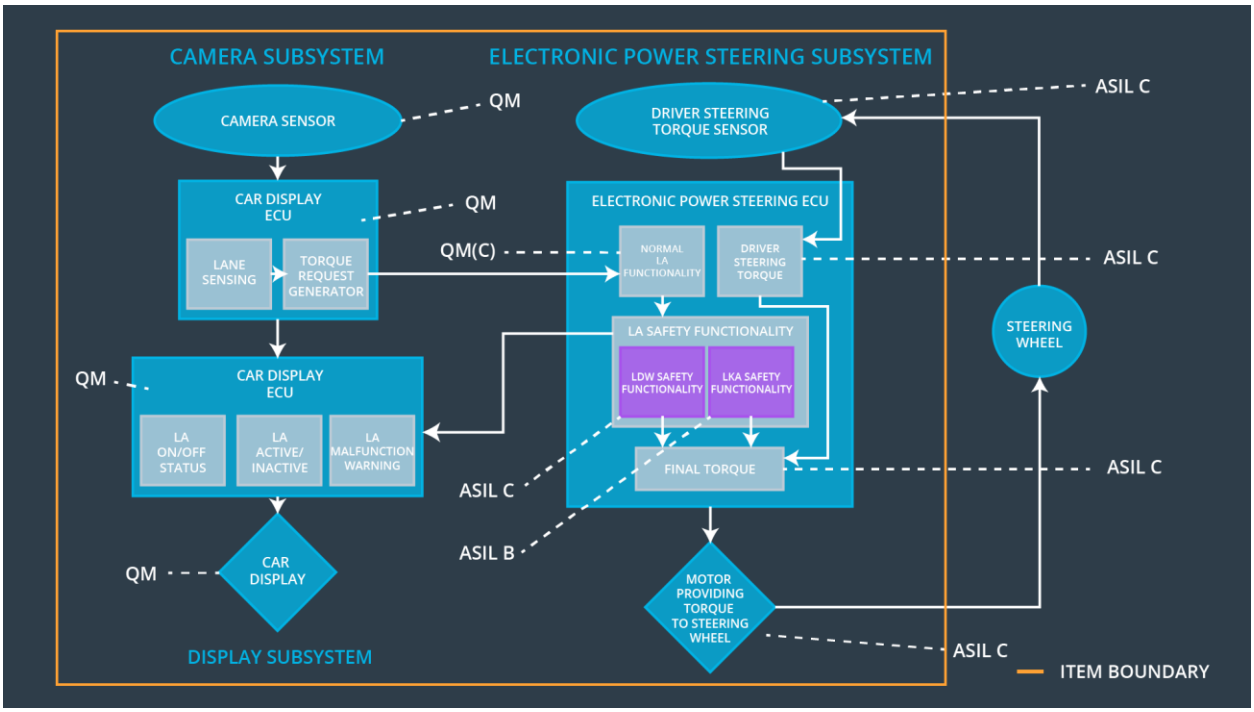
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The EPS ECU shall ensure that the LKA support is available for only Max_Duration	B	500 ms	Off

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	Do tests to ensure that the max_duration chosen really did dissuade drivers from taking their hands off the wheel.	Verify that the system really does turn off if the lane keeping assistance every exceeded max_duration.

Refinement of the System Architecture

[Instructions: Include the refined system architecture. Hint: The refined system architecture should include the system architecture from the end of the functional safety lesson including all of the ASIL labels.]



Allocation of Functional Safety Requirements to Architecture Elements

[Instructions: Mark which element or elements are responsible for meeting the functional safety requirement.]

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-01	The EPS ECU shall ensure that torque frequency for LDW shall not exceed amplitude Max_Torque_Amplitude	✕		
Functional Safety Requirement 01-02	The EPS ECU shall ensure that torque frequency for LDW shall not exceed frequency Max_Torque_Frequency	✕		
Functional Safety Requirement 02-01	The EPS ECU will ensure that the LKA function shall be time limited by making sure that the additional steering torque shall end after a given timer interval so that the driver cannot misuse the system for autonomous driving	✕		

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	Off	Torque frequency or amplitude exceeds its maximum threshold i.e., Max_Torque_Amplitude or Max_Torque_Frequency	Yes	LED on Car Display
WDC-02	Off	The LKA torque is being applied for more than max_duration	Yes	LED on Car Display