Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [2.0]

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.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description
08-06-2019	1.0	Vaidehi Venkatesan	Initial Draft
08-07-2019	2.0	Vaidehi Venkatesan	Proof-read + Updated the architecture diagram

Table of Contents

[Instructions: We have provided a table of contents. If you change the document structure, please update the table of contents accordingly. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In Google Docs, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]

Purpose of the Functional Safety Concept

[Instructions: Answer what is the purpose of a functional safety concept?]
The purpose of functional safety concept is to avoid accidents by reducing the risks to acceptable levels. Functional safety concept does a system architecture analysis to identify subsystems that are impacted by/ from the safety goals identified at the end of Hazard Analysis and Risk Assessment. It also defines the functional safety requirements for the subsystems along with functional safety attributes like targeted ASIL levels, Fault Tolerant Time Interval and Safe State definition.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

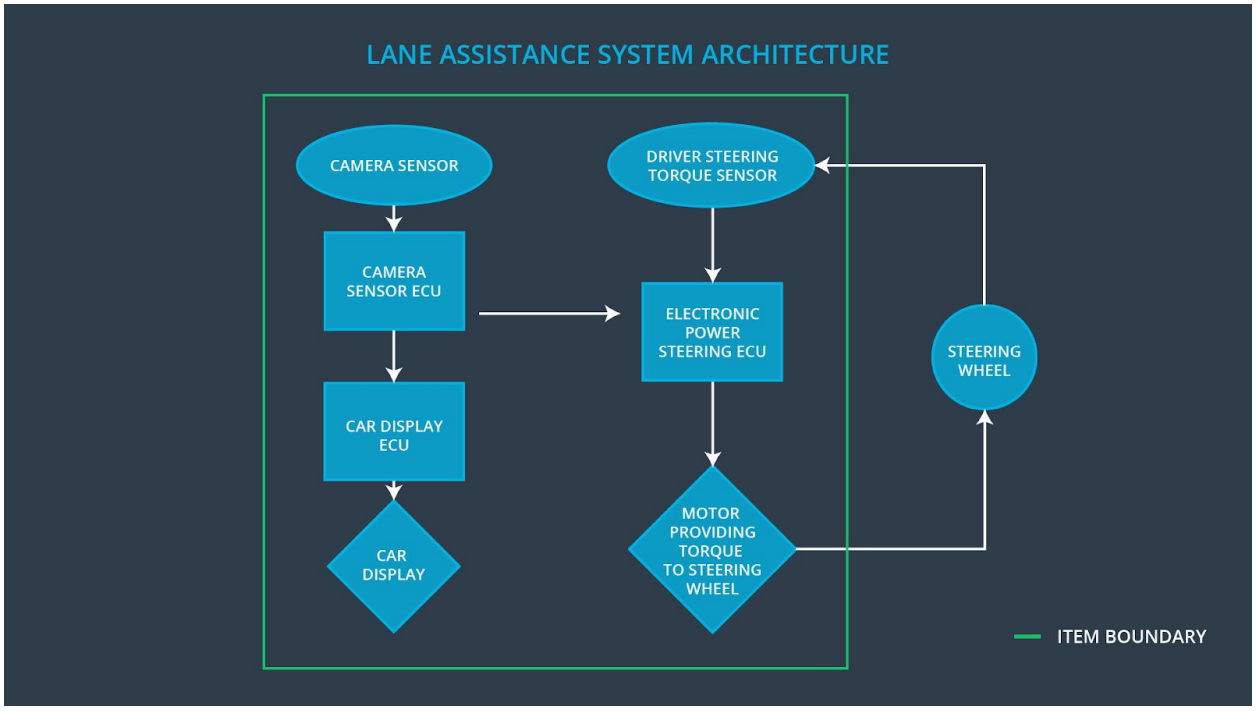
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

OPTIONAL:
If you expanded the hazard analysis and risk assessment to include other safety goals, include them here.
]

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.

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	Camera Sensor captures video feed of lane lines and scenes of the road in which the vehicle is driving and passes the information to Camera Sensor ECU.
Camera Sensor ECU	Camera Sensor ECU is responsible for detecting lane lines from the Camera Sensor inputs and determine when the vehicle leaves the lane by mistake. When the vehicle leaves the lane, it also informs the Car Display ECU.
Car Display	Car Display ECU gets input from Camera Sensor ECU with an indication that vehicle leaves the

	lane. It notifies Car Display ECU to turn on the departure warning in the car dashboard.
Car Display ECU	Car Display ECU is responsible for turning on / off the vehicle departure warning.
Driver Steering Torque Sensor	Responsible for measuring the steering torque from the steering wheel output. It communicates the observed torque information to the Electronic Power Steering ECU.
Electronic Power Steering (EPS) ECU	EPS ECU is responsible for getting inputs from the Camera Sensor and Driver Steering Torque Sensor in understanding if lane keeping function needs to be activated and a haptic feedback needs to be provided to the user for lane departure. EPS ECU also computes the compensating steering torque required to keep the vehicle in lane.
Motor	Motor receives input from EPS ECU to adjust the steering torque input 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	MORE	Oscillating steering

	Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback		torque is provided 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	Oscillating steering torque is provided 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	Steering torque applied is not limited to a time duration which leads to its 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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below MAX_Torque_Amplitude	C	50 ms	Oscillating torque is set to zero when a fault is detected.
Functional	The lane keeping item shall ensure that	C	50 ms	Oscillating

Safety Requirement 01-02	the lane departure oscillating torque frequency is below MAX_Torque_Frequency			torque is turned off when a fault is detected.

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	Oscillating torque amplitude < MAX_Torque_Amplitude is the acceptance criteria. Method: This value is chosen after conducting experiments with different amplitudes and testing how drivers react.	Acceptance criteria: When the torque amplitude crosses the MAX_Torque_Amplitude, the lane assistance output is set to zero within the 50 ms fault tolerant time interval. Method: Do a software test inserting a fault into the system and check if the system behaves within the acceptance criteria.
Functional Safety Requirement 01-02	Oscillating torque frequency < MAX_Torque_Frequency is the acceptance criteria. Method: This value is chosen after conducting experiments with different frequency and testing how drivers react.	Acceptance criteria: When the torque frequency crosses the MAX_Torque_Frequency, the lane assistance output is set to zero within the 50 ms fault tolerant time interval. Method: Do a software test inserting a fault into the system and check if the system behaves within the acceptance criteria.

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

Lane Keeping Assistance (LKA) Requirements:

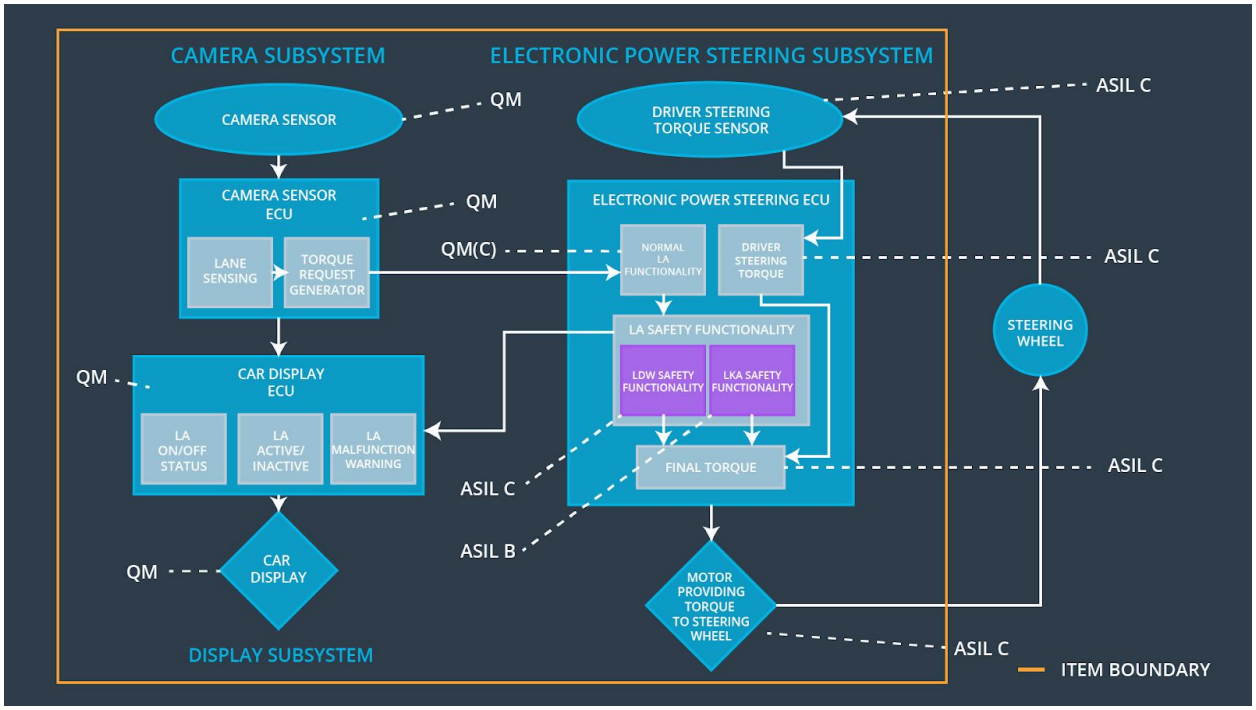
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration".	B	500 ms	Lane keeping assistance torque is set to zero and Lane keeping assistance system is turned 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	Duration when lane assistance is used at once should be at most max_duration only. Method: Experiments can be done to ensure that Max_duration applied dissuades drivers from taking their hands off the wheel.	Acceptance Criteria: Lane keeping function is shut off when duration exceeds max_duration Method: Do a software test inserting a fault into the system and check if the system behaves within the acceptance criteria.

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. 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 keeping item shall ensure that the lane departure oscillating torque amplitude is below MAX_Torque_Amplitude	Final electronic power steering torque system component provides the required adjustmen	**n/a**	**n/a**

		t to the 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	Final electronic power steering torque system component provides the required adjustment to the torque frequency	**n/a**	**n/a**
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration".	Final electronic power steering torque system component sets the torque to zero on reaching duration limit.	**n/a**	**n/a**

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 the functionality	Malfunction in Functional Safety Requirements 01-01, 01-02	Yes	The haptic feedback given to the user stops.
WDC-02	Turn off the functionality	Malfunction in Functional Safety Requirement 02-01	Yes	The driver will see a warning light on the dashboard when the system malfunctions.