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.

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
6 Feb 2018	1.0	Vilas Chitrakaran	Initial draft

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]

Document history

Table of Contents

Purpose of the Functional Safety Concept

Inputs to the Functional Safety Analysis

- Safety goals from the Hazard Analysis and Risk Assessment
- Preliminary Architecture
  - Description of architecture elements

Functional Safety Concept

- Functional Safety Analysis
- Functional Safety Requirements
- Refinement of the System Architecture

Allocation of Functional Safety Requirements to Architecture Elements
Warning and Degradation Concept

Purpose of the Functional Safety Concept

[Instructions: Answer what is the purpose of a functional safety concept?]
The Functional Safety Concept identifies which elements of the system are relevant to functional safety, identifies safety requirements for them, and allocates those requirements to appropriate sub-systems in the system architecture.

Inputs to the Functional Safety Concept

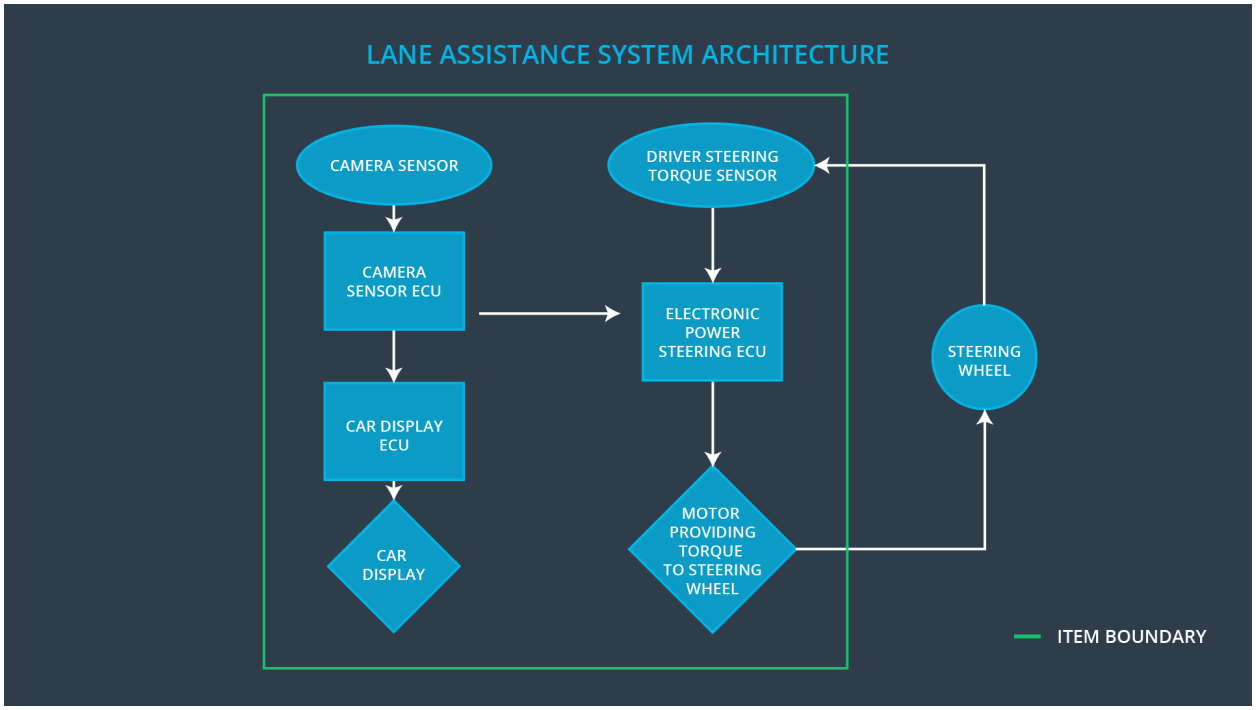
Safety goals from the Hazard Analysis and Risk Assessment

[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.
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 (LDW) function shall be limited
Safety_Goal_02	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 can not misuse the system for autonomous driving

Preliminary Architecture

[Instructions: Provide a preliminary architecture for the lane assistance item. Hint: See Lesson 3: Item Definition]
A high level system architecture of the Lane Assistance item is as follows



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 video stream of the environment ahead of the vehicle.
Camera Sensor ECU	Applies computer vision algorithms to detect lane lines, computes ego-position of the vehicle relative to the lane lines, detects the event of the vehicle leaving the lane unintentionally, and computes corrective steering torque request.
Car Display	Displays status information, warnings and faults to the driver, and is driven by the Car Display ECU
Car Display ECU	Processes messages from the Camera Sensor ECU and the Electronic Power Steering ECU to determine the status (on/off) of the LA system, whether the system is active or not, and whether there are any malfunctions warnings that must be shown
Driver Steering Torque Sensor	Detects and measures steering torque applied by the

	driver
Electronic Power Steering ECU	Processes control signals from the Camera subsystem, generates steering torque signal that drives the steering wheel motor.
Motor	Actuator that provides a physical feedback to the user in the form of oscillating or sustained steering torque.

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

[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	50ms	Function turned 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	50ms	Function turned 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	● Criteria: Validate that Max_Torque_Amplitude provides sufficient haptic feedback and is well within limits to allow drivers to maintain control of the vehicle. ● Method: Validation trial conducted on the test track on a	● Criteria: Verify that steering oscillating torque does not exceed Max_Torque_Amplitude ● Method: Instrument the system with torque measuring equipment, initialise system to trigger the function and

	statistically significant sample set of drivers from the target demographic.	measure maximum steering torque output.
Functional Safety Requirement 01-02	• Criteria: Validate that Max_Torque_Frequency provides sufficient haptic feedback and is well within limits to allow drivers to maintain control of the vehicle. • Method: Validation trial conducted on the test track on a statistically significant sample set of drivers from the target demographic.	• Criteria: Verify that steering oscillating torque does not exceed Max_Torque_Frequency • Method: Instrument the system with torque measuring equipment, initialise system to trigger the function and measure maximum steering torque output.

[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	500ms	Function turned off

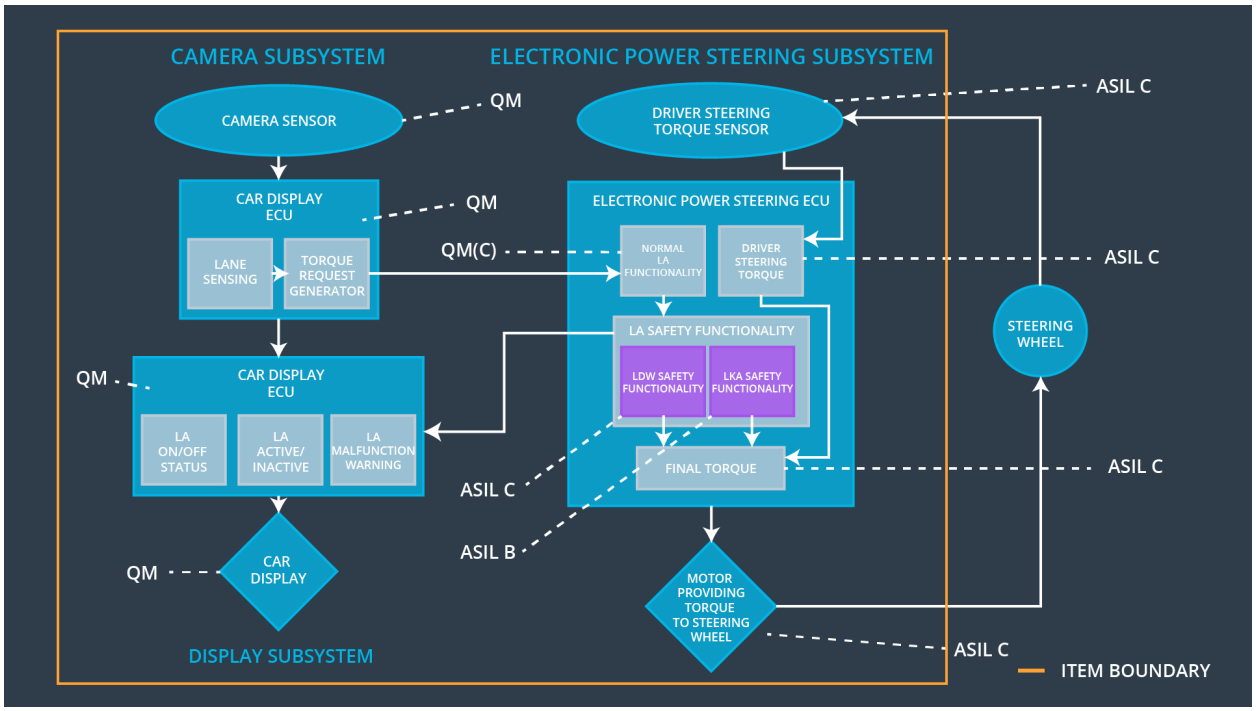
Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement 02-01	• Criteria: Validate that the Max_Duration chosen really did dissuade drivers from taking their hands off the wheel.	• Criteria: Verify that the lane keeping function really does turn off after Max_Duration • Method: Instrument the system with time measuring

	• Method: Validation trial conducted on the test track on a statistically significant sample set of drivers from the target demographic.	equipment, initialise system to trigger the function and measure time duration until the function is turned off.

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.]



The refined system architecture is shown above with component ASILs identified for functional safety of the item.

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	Camera	Car Display

		Power Steering ECU	ECU	ECU
Functional Safety Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	**X**		
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 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

[Instructions: Fill in the warning and degradation concept.]

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Function turned off.	On detection of malfunction causing steering torque amplitude or frequency to exceed limits	Yes	Warning light on dashboard to notify when disabled
WDC-02	Function turned off.	On detection of malfunction causing steering torque duration to exceed limit.	Yes	Warning note in the driver's manual to not use LKA function for autonomous driving