Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [Version 1.0]
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
2019/2/27	1.0	Harrison Hou	Initial version
2019/3/2	1.1	Harrison Hou	Update the document according to the guidance video from Silver: - Description of the architecture elements

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 a functional safety concept is to identify new requirements and allocate these requirements to system diagrams at a functional level. The functional safety concept is looking at the item at a high level. It does not go into technical details. It only looks at a general functionality of the item.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

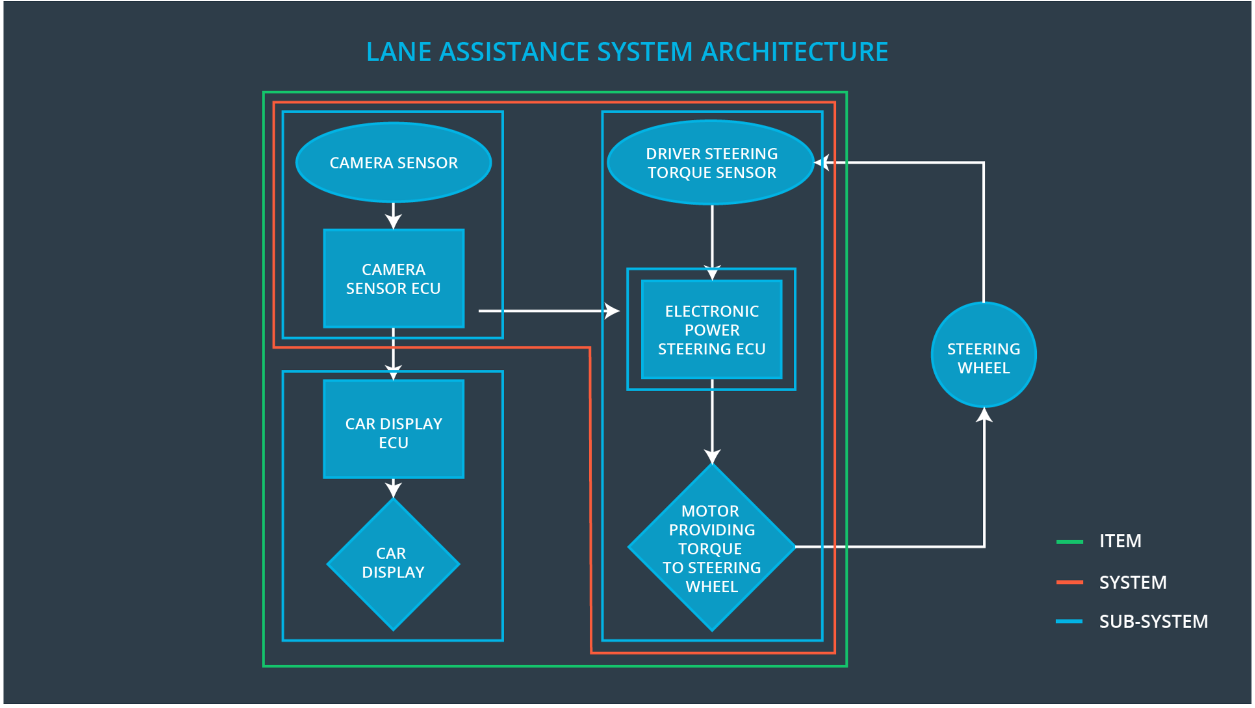
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

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 as autonomous driving.
Safety_Goal_03	The oscillating steering torque from the lane departure warning function shall be strong enough for the driver to feel.
Safety_Goal_04	The lane keeping assistance function shall be activated only with unintended ego lane deviation.

Preliminary Architecture

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


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
SYSTEM
SUB-SYSTEM

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 sensors get the picture of the road
Camera Sensor ECU	ECU determine lane departures and tells the steering wheel how hard to turn and tells the car display system what to display
Car Display	Display warnings
Car Display ECU	Receive warning signal from camera ECU and determines whether to display and what to display.
Driver Steering Torque Sensor	Sense how hard the driver move the steering wheel
Electronic Power Steering ECU	Gets the hard to turn steering wheel from camera ECU and from driver steering torque sensor, then output the

	desired torque to steering wheel.
Motor	Operate the torque request.

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	No	The lane keeping assistance function is not limited in time duration which

	when active in order to stay in ego lane		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	Turn the lane departure warning function 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	Turn the lane departure warning function 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	For whatever value we end up choosing for the max torque amplitude, we need to **validate** that we chose a reasonable value. We would need to test how drivers react to different torque amplitudes to prove that we chose an appropriate value.	We then need to **verify** that the safety requirement is met; when the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50ms fault tolerant time interval. For this specific case, we would probably do a software test inserting a fault into the system and seeing what happens.
Functional Safety	For whatever value we end up choosing for the max torque	We then need to **verify** that the safety requirement is met; when the

Requirement 01-02	frequency, we need to **validate** that we chose a reasonable value. We would need to test how drivers react to different torque frequency to prove that we chose an appropriate value.	torque frequency crosses the limit, the lane assistance output is set to zero within the 50ms fault tolerant time interval. For this specific case, we would probably do a software test inserting a fault into the system and seeing what happens.

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

Lane Keeping Assistance (LKA) Requirements:

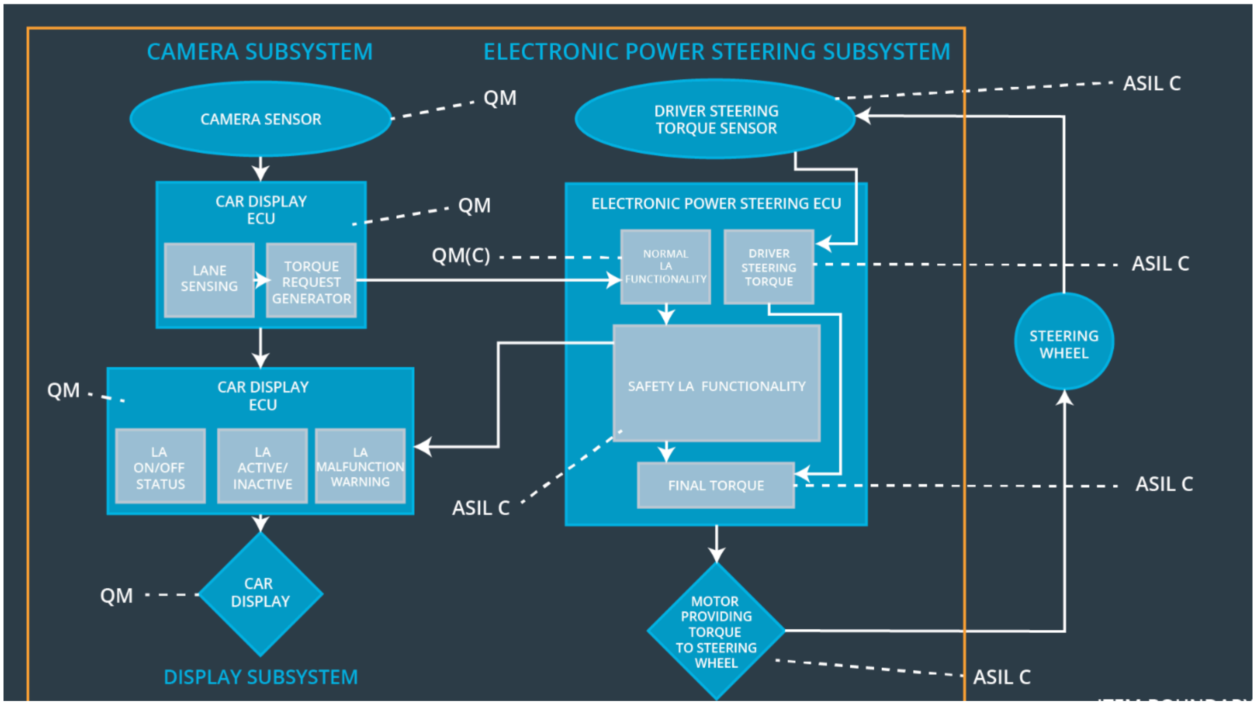
ID	**Functional Safety Requirement**	**ASIL**	**Fault Tolerant Time Interval**	**Safe State**
Functional Safety Requirement 02-01	the electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500ms	Turn the lane keeping assistance torque to 0.

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	For the lane keeping assistance function, we would have to test and validate that the max_duration chosen really did dissuade drivers from taking their hands off the wheel.	Then we would 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. 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.	**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	Turn off the functionality	The lane departure oscillating torque amplitude or frequency is above Max_Torque_Amplitude or Max_Torque_Frequency.	Y	Turn on a warning light on the dashboard when the system malfunctions.
WDC-02	Turn off the functionality	The lane keeping assistance torque is applied for more than Max_Duration	Y	Turn on a warning light on the dashboard when the system malfunctions.