Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [Version]

Document history

Date	Version	Editor	Description
02.09.2017	1.0	Klemens Esterle	Initial Version

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 functional safety concept is used to define functional safety requirements looking at the general functionality of the item.

Inputs to the Functional Safety Concept

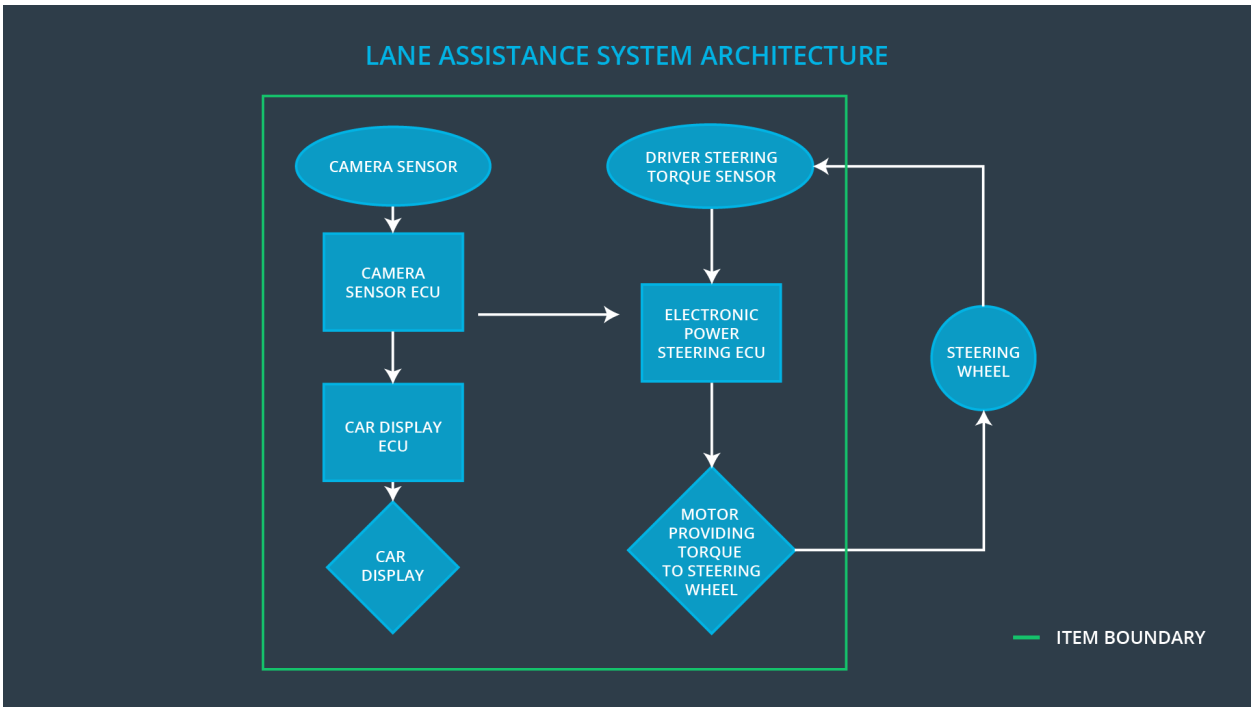
Safety goals from the Hazard Analysis and Risk Assessment

[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 osciallating 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



Description of architecture elements

Element	Description
Camera Sensor	Front camer sensor to film lane in front
Camera Sensor ECU	ECU using algorithms to extract lane information from camera video stream
Car Display	Interface to human showing current status of functionality (on, off)
Car Display ECU	ECU to process input from driver (swtich off) and also process any system status for visualization to driver
Driver Steering Torque Sensor	Sensor to measure applied steering torque by driver to steering wheel
Electronic Power Steering ECU	ECU to process request for returning to lane and sending necessary torque signal to motor
Motor	Actuator applying torque to 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

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.
Malfunction_04	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	WRONG	The lane keeping assistance function is active, but there is high uncertainty about the lane detection result,

			leading to a wrong stabilization actuation.

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 electronic power steering ECU shall ensure that the lane departure warning oscilatting torque amplitude is below Max_Torque_Amplitude	C	50ms	System turned off
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure warning oscilatting torque frequency is below Max_Torque_Frequency	C	50ms	System 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	test how drivers react to different torque amplitudes	Software-In-The-Loop tests with fault insertion: desired torque amplitude signal is above limit -→ does Motor ECU limits torque to specified value?
Functional Safety Requirement 01-02	test how drivers react to different torque frequencies	Software-In-The-Loop tests with fault insertion: desired torque frequency signal is above limit-→ does Motor ECU limits torque to specified value?

Lane Keeping Assistance (LKA) Requirements:

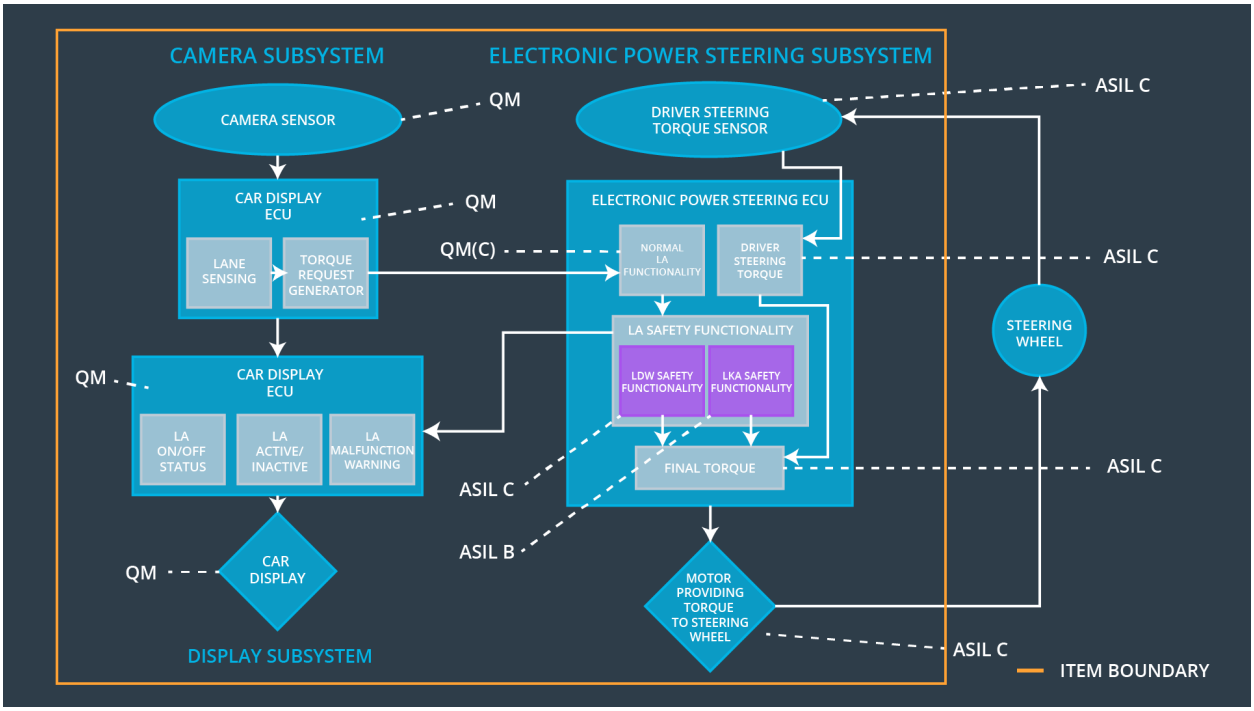
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500ms	System turned off
Functional Safety Requirement 02-02	The camera sensor ECU shall ensure that the system is switched off if the detection uncertainty is below Min_Detection_Certainty	B	50ms	System 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	test and validate that the max_duration chosen really did dissuade drivers from taking their hands off the wheel	Software-In-The-Loop tests with fault insertion: no torque applied by human for more than 500ms
Functional Safety Requirement 02-02	Test wether degradation method will result in robust state	Software-In-The-Loop tests with fault insertion: detection certainty below Min_Detection_Certainty → is return safe for various scenarios with typical driver behavior?

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 electronic power steering ECU shall ensure that the lane departure warning oscilatting torque amplitude is below Max_Torque_Amplitude	**x**		
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure warning oscilatting torque frequency is below Max_Torque_Frequency	**x**		
Functional	The electronic power steering	**x**		

Safety Requirement 02-01	ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration			
Functional Safety Requirement 02-02	The camera sensor ECU shall ensure that the system is switched off if the detection uncertainty is below Min_Detection_Certainty	**x**	**x**	**x**

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off functionality	Malfunction_01, Malfunction_02	yes	warning light on the dashboard
WDC-02	Turn off functionality	Malfunction_03	yes	warning light on the dashboard, acoustic signal
WDC-03	Gradual degredation	Malfunction_04	yes	warning light on the dashboard, acoustic signal