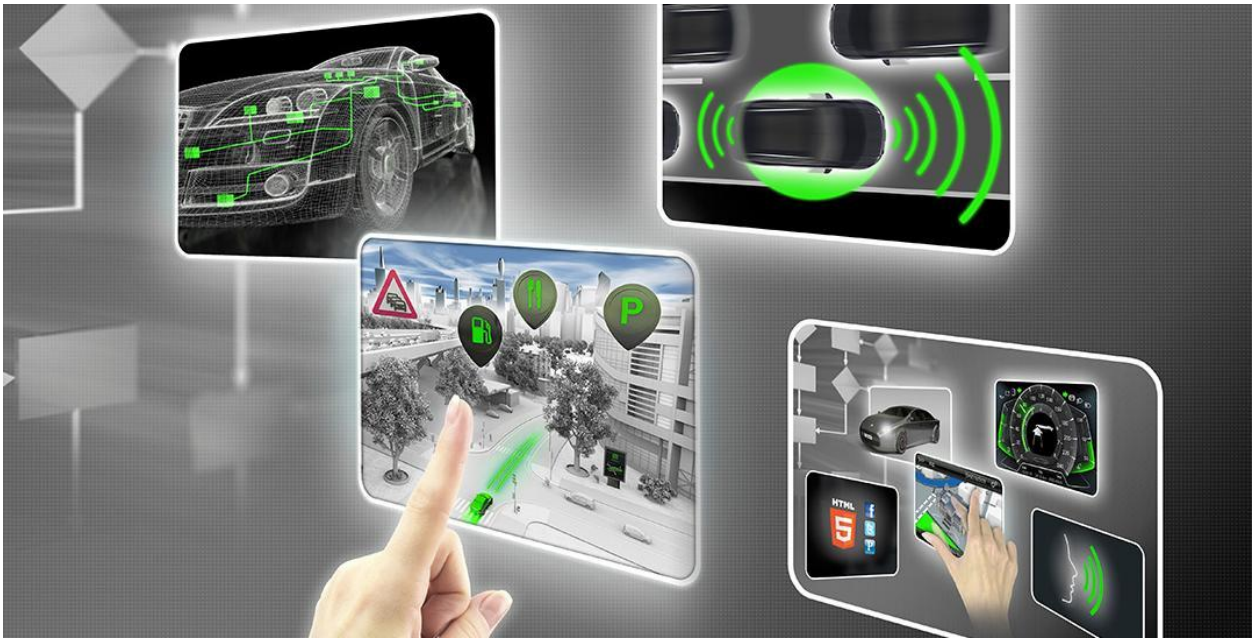
Elektrobit

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
19-Dec-2017	1.0	Carsten MIELENZ	1st 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 allocates the Safety Goals of the Hazard analysis & risk assessment to relevant Systems of the item. The Safety Goal for a relevant System is further refined into Functional Safety Requirements.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

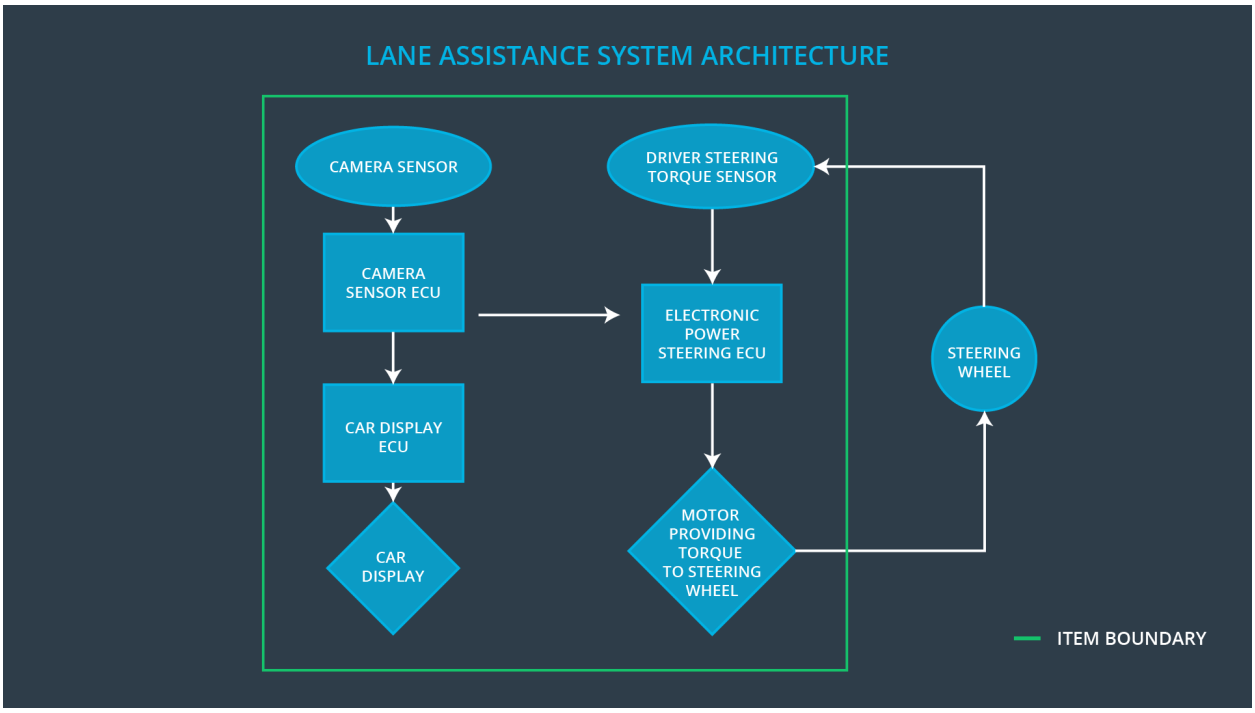
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

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	The Camera Sensor takes the picture of the lane and send it to the Camera Sensor ECU.
Camera Sensor ECU	The Camera Sensor ECU senses the lane picture for lane departure. In case of lane departure, it creates a torque request which is sent to the Electronic Power Steering ECU. It also sends a lane departure info to the Car Display ECU for this case.
Car Display	The Car Display displays lane departure info.
Car Display ECU	The Car Display ECU analyzes the lane departure info from the Camera Sensor ECU and send a lane departure info display request to the Car Display
Driver Steering Torque Sensor	The Driver Steering Torque Sensor the turning of the Steering Wheel and sent the measurement to the Electronic Power Steering ECU.

Electronic Power Steering ECU	The Electronic Power Steering ECU calculates the torque value for the Motor based on the measurement from the Driver Steering Torque Sensor and the torque request from the Camera Sensor ECU.
Motor	The Motor provides torque to the Steering Wheel based on value which was provided by the Electronic Power Steering ECU

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	LDW function is giving MORE torque as it is safe	The LWD 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	LDW function is giving MORE torque as it is safe	The LWD function applies an oscillating torque with very high torque frequency (above limit)
Malfunction_03	Lane Keeping Assistance (LKA)	The LKA function provides NO time	The LKA function is not limited in time

	function shall apply the steering torque when active in order to stay in ego lane	limit of usage	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	Zero torque
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	Zero torque

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	Check that the selected Max_Torque_Amplitude is reasonable for the driver to still control the vehicle.	Check that in case the torque amplitude crosses the Max_Torque_Amplitude the LDW sets torque to zero within 50ms
Functional Safety Requirement 01-02	Check that the selected Max_Torque_Frequency is reasonable for the driver to still control the vehicle.	Check that in case the torque frequency crosses the Max_Torque_Frequency the LDW sets torque to zero within 50ms

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

Lane Keeping Assistance (LKA) Requirements:

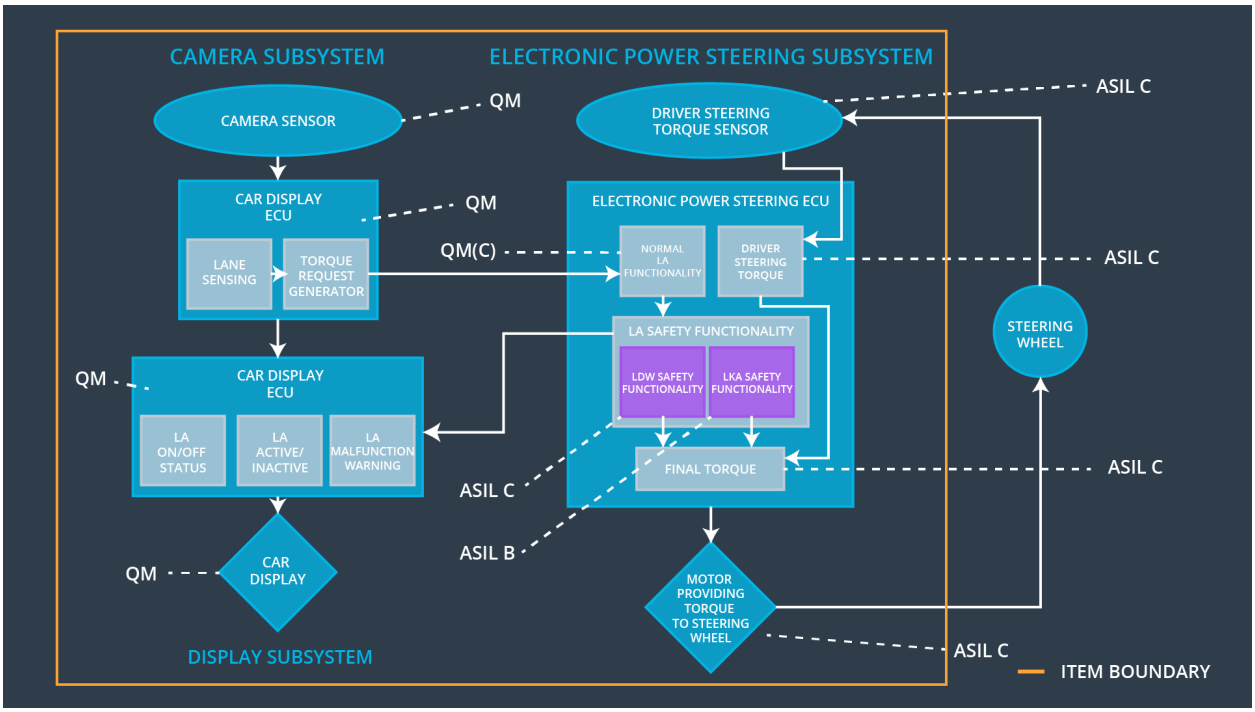
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	Lane keeping assistance function shall be time limited and the additional steering torque shall end after a given timer interval Max_Duration so that the driver cannot misuse the system for autonomous driving	B	500ms	Zero Torque

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	Check that the selected Max_Duration value sufficient to prevent drivers to take off their hands from the steering wheel.	Check that the system turns off if the LKA function exceeded the Max_Duration with 500ms

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 oscillating torque amplitude is below Max_Torque_Amplitude	**X**		
Functional Safety Requirement 01-02	The electronic power steering ECU 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 function	Malfunction_01 or Malfunction_02	Yes	Lane Assist Malfunction
WDC-02	Turn-off function	Malfunction_03	Yes	Lane Assist not designed for autonomous driving