Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
24.5.2018	1.0	Arindam Baidya	First Attempt

Table of Contents

Purpose of the Functional Safety Concept

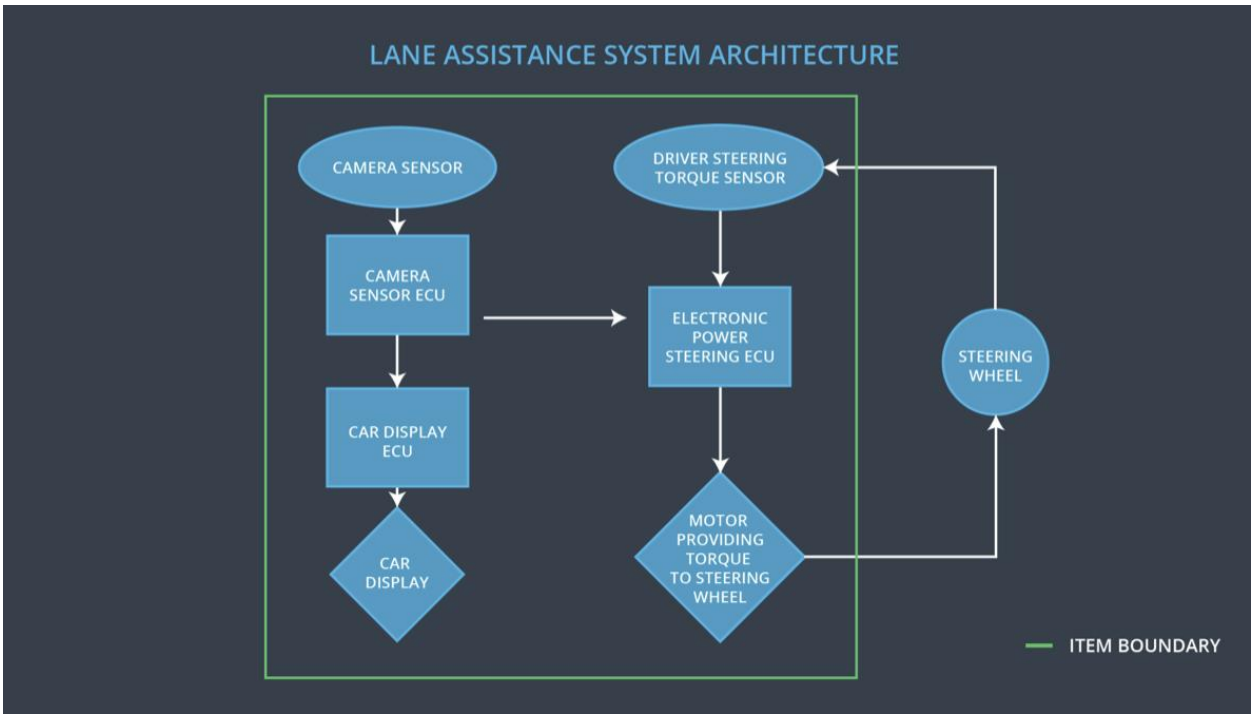
Functional safety concept is looking at the item from a higher level, without going into technical details. The purpose of functional safety concept is to avoid accidents by reducing risks to acceptable levels.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

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 additional steering torque shall end after a given time interval so that the driver cannot misuse the system for autonomous driving.
Safety_Goal_03	The Lane Departure Warning function shall be deactivated when the camera sensor or any other sensors start malfunctioning.
Safety_Goal_04	Lane Keeping Assistance has to be sensible to different coloring of lane lines, and reliably detect and react on merging lanes in advance

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Captures images from the road and provide them to Camera Sensor ECU
Camera Sensor ECU	Analyses lane line position from the camera images and generates a torque request to the Electronic Power Steering ECU.
Car Display	Displays warning, feedback and Lane Departure Assistance status to the driver
Car Display ECU	Drive the Car Display component to show the Lane Keep Assistance warning and Lane Departure Assistance status
Driver Steering Torque Sensor	Measure and deliver the steering torque intensity provided by the driver to Electronic Power Steering ECU

Electronic Power Steering ECU	Use the information received from Camera Sensor ECU and Driver Steering Torque Sensor and torque requested by the LKA and LDW and computes the necessary torque to be applied by the Motor actuator
Motor	Receives final torque to be calculated by Electronic Power Steering ECU and applies it 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

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	NO	The lane keeping assistance function is not limited in time duration which leads to misuse as

	to stay in ego lane		an autonomous driving function.
Malfunction_04	The Lane Departure Warning function shall deactivate when the camera sensor or any other sensors start malfunctioning.	WRONG	The Lane Departure Warning function starts reacting randomly when the camera sensor or any other sensors start malfunctioning.
Malfunction_05	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	WRONG	Camera sensor does not detect yellow lanes of construction site and therefore does not detect lane merging situations correctly. While Keeping the lane LKA introduces lane merging without further precautions.

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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Lane Assistant functionality 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	Lane Assistant functionality off
Functional Safety Requirement 01-03	The LDW function shall be deactivated when the camera sensor or any other sensor starts malfunctioning.	C	10ms	LDW Function is deactivated

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 to prove that an appropriate value was chosen.	Verify that system turns off if LDW ever exceeds Max_Torque_Amplitude.
Functional Safety Requirement 01-02	Test how drivers react to different torque frequencies to prove that an appropriate value was chosen.	Verify that system turns off if LDW ever exceeds Max_Torque_Frequency.
Functional Safety Requirement 01-03	Validate Lane Departure Warning is off when the camera sensor or any other sensor is malfunctioning.	Verify the LDW is never on when camera sensor or any other sensors is malfunctioning.

Lane Keeping Assistance (LKA) Requirements:

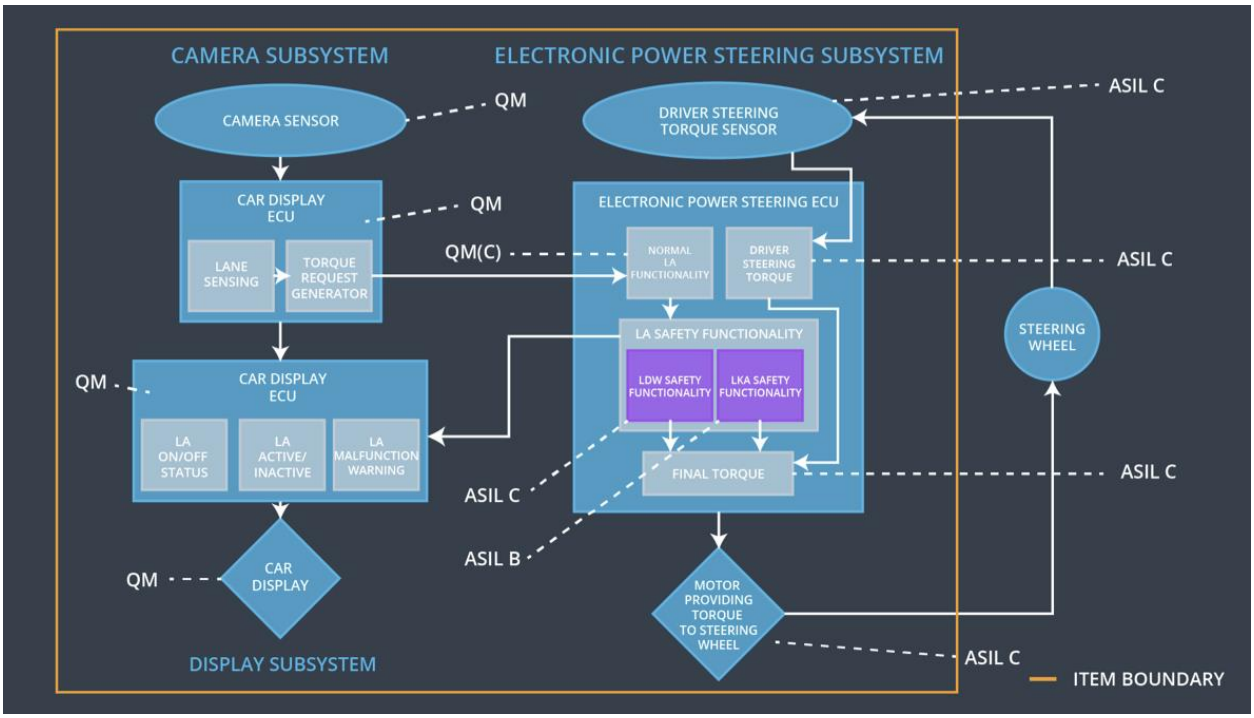
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500ms	Lane Assistant functionality off
Functional Safety Requirement 02-02	The camera sensor ECU shall not request torque if Laneline_Is_Yellow is stated true by camera sensor ECU.	D	30ms	Lane Assistant functionality off

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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement	Test and validate that the Max_Duration chosen really dissuades drivers from taking their hands off the wheel.	Verify that system turns off if LKA ever exceeds MAX_DURATION.

02-01		
Functional Safety Requirement 02-02	Test and validate that Laneline_Is_Yellow is stated correctly, if lanelines turn yellow.	Verify that system turns off if Lane_Not_Found is true.

Refinement of the System Architecture



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	The electronic power steering ECU shall ensure that the lane	**x**		

Requirement 01-01	departure oscillating torque amplitude is below Max_Torque_Amplitude			
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 01-03	The Lane Departure Warning function shall be deactivated when the Electronic Power Steering ECU detects camera sensor or any other sensor has started malfunctioning	**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**		
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that lane keeping assistance torque is zero if camera sensor ECU states Laneline_Is_Yellow is true	**x**		

Warning and Degradation Concept

ID	**Degradation Mode**	**Trigger for Degradation Mode**	**Safe State invoked?**	**Driver Warning**
WDC-01	Turn off Lane Assistant functionality	Malfunction_01	Yes	Lane Departure Warning Malfunction Warning on Car Display
WDC-02	Turn off Lane Assistant	Malfunction_02	Yes	Lane Departure Warning

	functionality			Malfunction Warning on Car Display
WDC-03	Turn off Lane Assistant functionality	Malfunction_03	Yes	Lane Keeping Assistance Malfunction Warning on Car Display
WDC-04	Turn off Lane Assistant functionality	Malfunction_04	Yes	Lane Departure Warning Malfunction Warning on Car Display
WDC-05	Turn off Lane Assistant functionality	Malfunction_05	Yes	Lane Keeping Assistance Malfunction Warning on Car Display