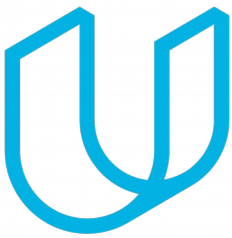
Elektrobit



UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
11/28/18	1.0	Kapy Kangombe	First draft of functional safety concept

Table of Contents

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

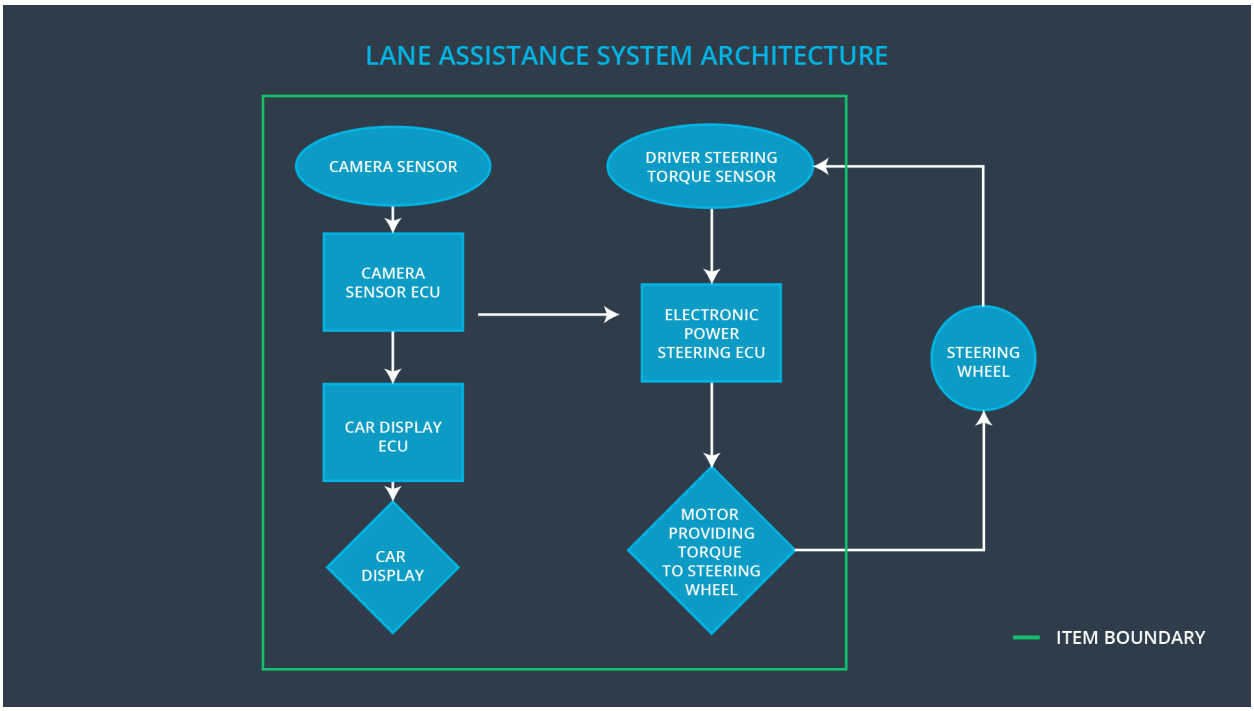
The purpose of the functional safety concept is to refine the safety goals established in the Hazard Analysis and Risk Assessment into functional safety requirements. These requirements define the vehicle's functions. The functional safety concept involves allocating the safety requirements to the relevant parts of the system diagram, refining the diagram, and ultimately proving that the system actually meets the requirements.

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 (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 time interval so that the driver cannot misuse the system for autonomous driving.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	A sensor that detects lane departures.
Camera Sensor ECU	A small computer that contains the hardware and software required for deep learning or for computer vision techniques like the Hough transform.
Car Display	A screen that displays a warning of the vehicle lane departure to the driver and also shows the status (on/off) of the the lane keeping function.
Car Display ECU	A small computer that contains the hardware and software to receive sensor data and display a warning of the vehicle lane departure to the driver. Also sends torque requests to the Electronic Power Steering ECU.
Driver Steering Torque Sensor	A sensor that detects how much the driver is turning the steering wheel.
Electronic Power Steering ECU	A small computer that contains the hardware and software required to receive sensor data and tell the motor how much torque to provider to the steering wheel. This is also where torque limits are applied.
Motor	Provides torque to the steering wheel to help the driver move the vehicle back towards the center of the lane.

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.

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 oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	LDW will set the oscillating torque amplitude to 0
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	LDW will set the oscillating torque amplitude to 0

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 to validate that Max_Torque_Amplitude is a reasonable value. Test how drivers react to different torque amplitudes to prove that we chose an appropriate Max_Torque_Amplitude value	Confirm that when the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms 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 Requirement 01-02	Test to validate that Max_Torque_Frequency is a reasonable value. Test how drivers react to different torque frequencies to prove that we chose an appropriate Max_Torque_Frequency value	Confirm that when the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms 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.

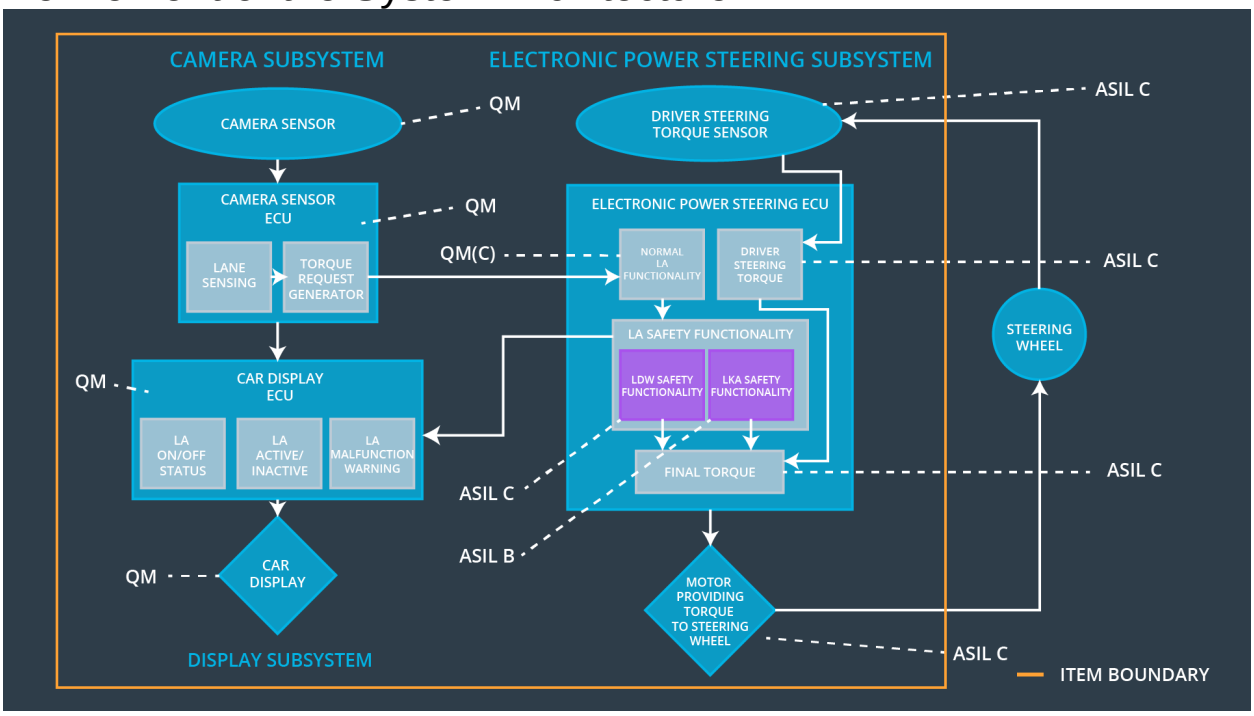
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	Electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500 ms	LKA will set the oscillating torque amplitude 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	Test to validate that the Max_Duration chosen really did dissuade drivers from taking their hands off the wheel	Confirm that the system really does turn off if the lane keeping assistance every exceeds Max_Duration and that the safe state is reached within the 500 ms fault tolerant time interval.

Refinement of the System Architecture



Allocation of Functional Safety Requirements to Architecture Elements

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 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 warning oscillating torque frequency is below Max_Torque_Frequency	**X**		
Functional Safety Requirement 02-01	Electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	**X**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW function	LDW malfunction	Yes	LDW malfunction warning light on dashboard
WDC-02	Turn off LKA function	LKA malfuntion	Yes	LKA malfunction warning light on dashboard