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
07-11-2018	1.0	Rasmita Samantaray	Initial Release

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

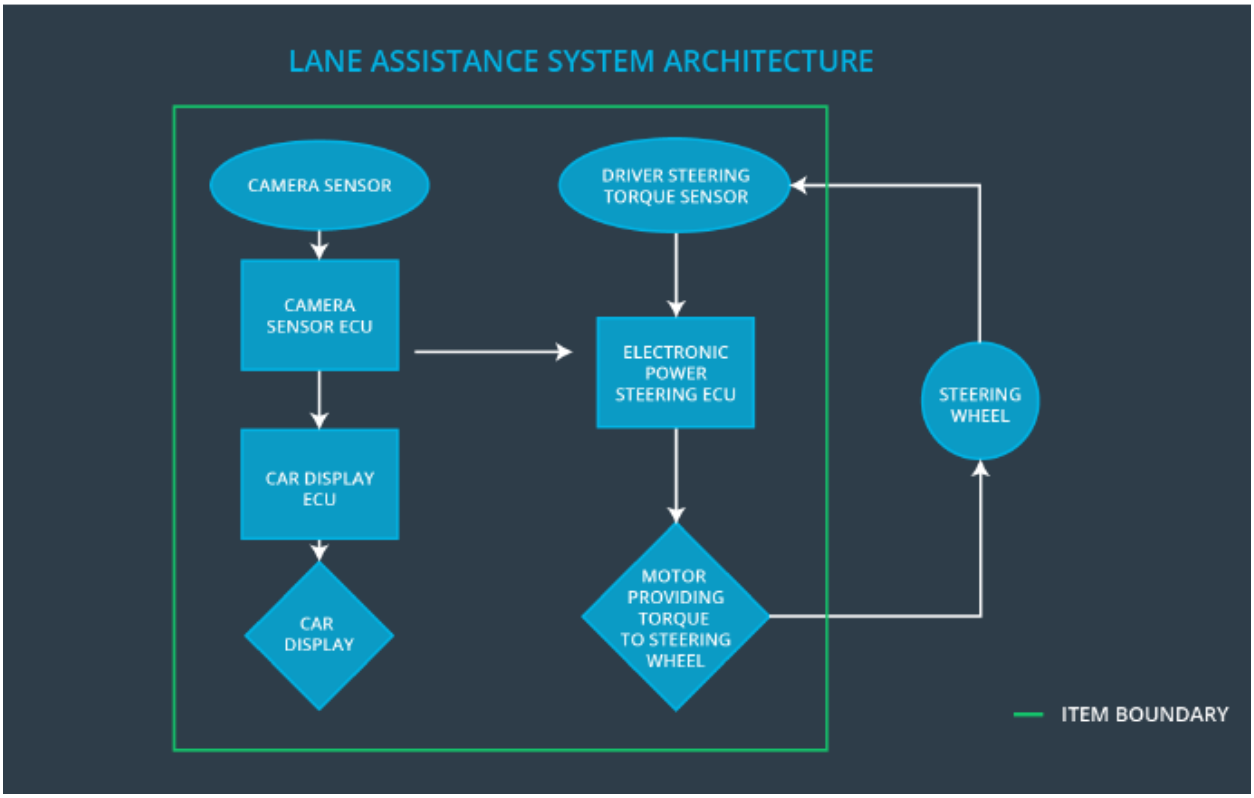
A functional safety concept generates functional safety requirements from the general functional safety goals. These requirements are allocated to subsystems and parts of the system. The system architecture may require modification to meet the functional safety requirements. Each of the requirements has attributes relating to the ASIL level, the fault tolerant time interval and the safe state of the system. Verification and validation of the requirements are discussed. The functional safety concept reviews general functionality of an item but does not include the technical implementation of the design.

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.
Safety_Goal_03	The lane detection shall not be activated if the detection for a certain environment is not reliable.
Safety_Goal_04	The lane keeping assistance (LKA) function shall deactivate when the camera sensor stops detecting road markings and shall warn the driver of its deactivation.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Physical sensor responsible for detecting lane lines
Camera Sensor ECU	Electronics hardware and processor or micro-controller responsible for interpreting camera data, identifying lane markings, determining vehicle position and issuing torque requests to the electronic power steering ECU
Car Display	Visual display responsible to displaying warning of lane departures and LKA and LDW activation and deactivations.
Car Display ECU	Electronics hardware responsible for interpreting input from other systems and controlling the lights or display unit.

Driver Steering Torque Sensor	Physical sensor such as an encoder or strain gauge capable of measuring steering torque input on the steering wheel from the driver.
Electronic Power Steering ECU	Depending on the required torque and the current torque, determines the additional torque to be applied to the steering and sends the value to the motor.
Motor	Based on the data sent by the Electronic Power Steering ECU, a torque is applied to the steering.

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). Driver might lose control of the vehicle.
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic	MORE	The lane departure warning function applies an oscillating torque with very high torque **frequency** (Above limit). Driver

	feedback		might lose control of the vehicle.
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 lane keeping item shall ensure that the lane departure warning torque amplitude is below Max_Torque_Amplitude	C	50 ms	Turn off LDW
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure warning torque frequency is below Max_Torque_Frequency	C	50 ms	Turn off LDW

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	Set oscillating torque amplitude to Max_Torque_Amplitude causes the light warning to be turned on	When the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval.
Functional Safety Requirement 01-02	Set oscillating torque frequency to Max_Torque_Frequency causes the warning light to be turned on	when the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval

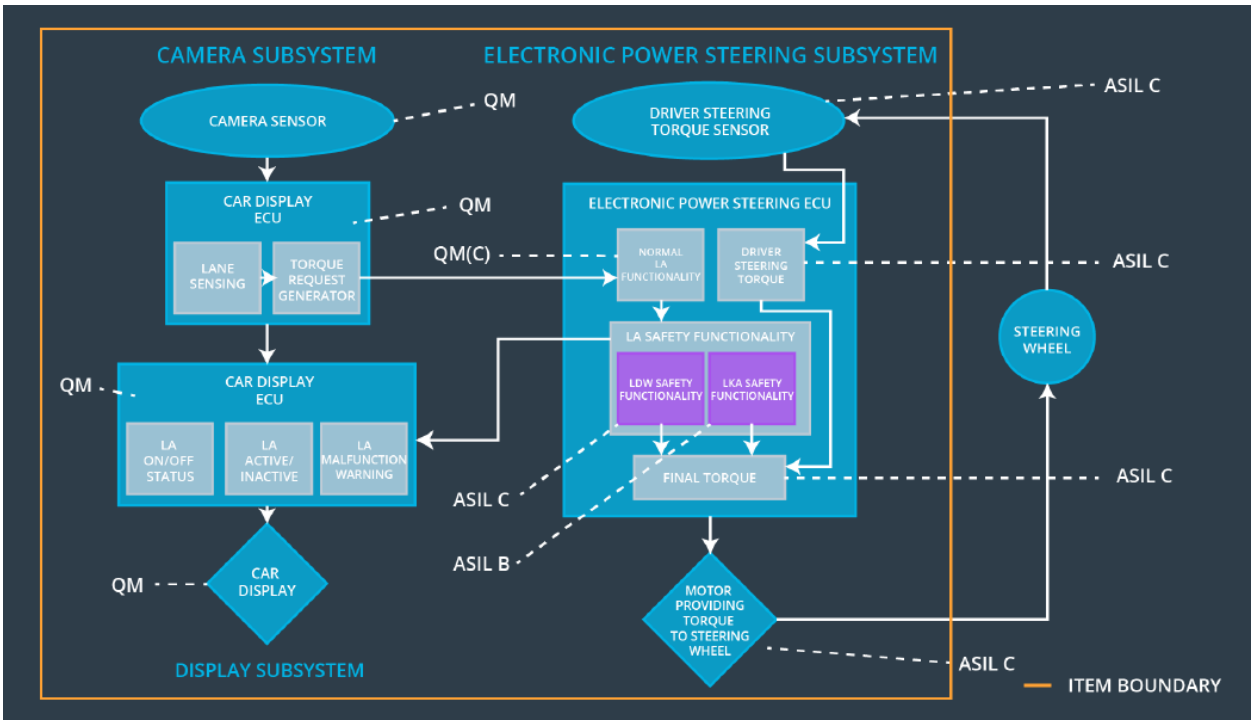
Lane Keeping Assistance (LKA) Requirements:

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	500 ms	Turn off LKA

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	Let the LKA active until the Max_Duration, and the warning light has to be turned on	when the time duration exceeds the limit, the lane assistance output is set to zero 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 lane keeping item shall ensure that the lane departure warning torque amplidute is below Max_Torque_Amplitude.	**X**		
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure warning 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

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	turn off the function	Is_Max_Torque_ Exceeded	Yes	Turn on warning light on car display
WDC-02	turn off the function	Is_Max_Duration _Exceeded	Yes	Turn on warning light on car display