Functional Safety Concept Lane Assistance

Document Version: 1.0

Submission Version 1.0, Released on 2018-01-28

Document history

Date	Version	Editor	Description
2018-01-28	1.0	Ioannis Tornazakis	First submission

Table of Contents

Purpose of the Functional Safety Concept

The purpose of this document is to refine the safety goals into high level functional safety requirements. Allocate these requirements to the parts of the system architecture that will implement them and expand the system architecture if needed to satisfy the safety requirements. Finally, prove that the system meets these requirements by setting the appropriate verification and validation criteria and methods.

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 the additional steering torque shall end after a given time interval so the driver cannot misuse the system for autonomous driving

Preliminary Architecture

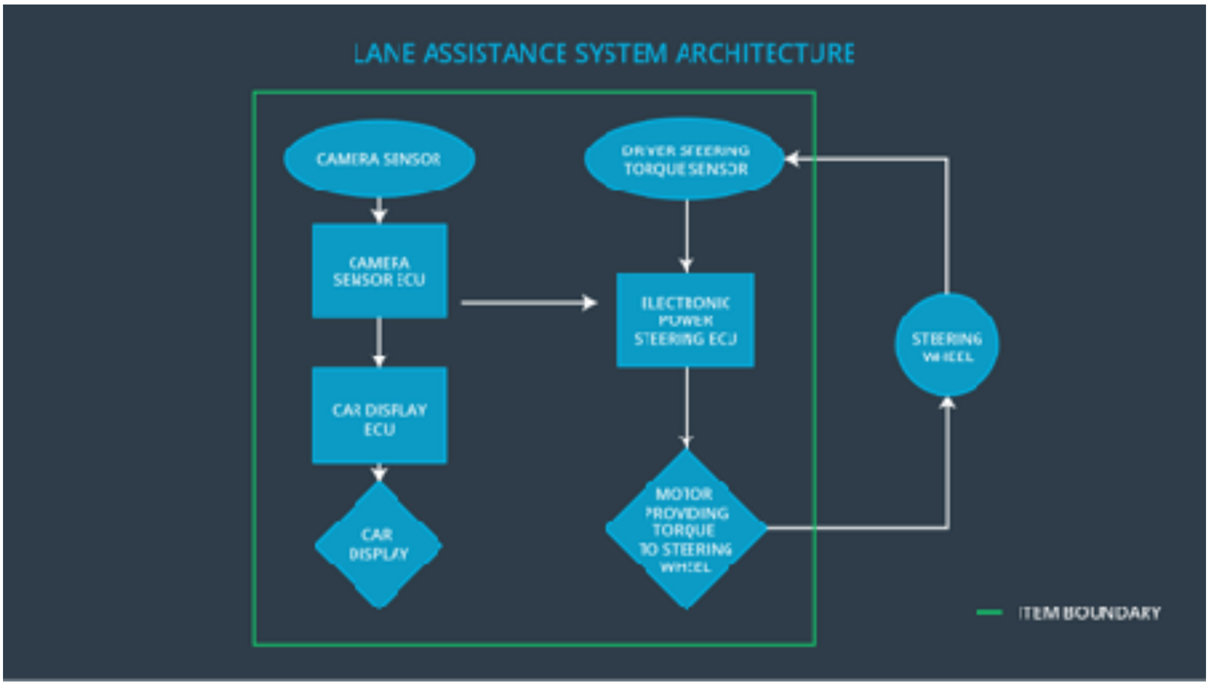
LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
DRIVER STEERING TORQUE SENSOR
CAMERA SENSOR ECU
ELECTRONIC POWER STEERING ECU
STEERING WHEEL
CAR DISPLAY ECU
CAR DISPLAY
MOTOR PROVIDING TORQUE TO STEERING WHEEL
ITEM BOUNDARY

FIGURE 1. LANE ASSISTANCE SYSTEM PRELIMINARY ARCHITECTURE

Description of architecture elements

Element	Description
Camera Sensor	Captures images of the road in front of the vehicle and sends them to the Camera ECU
Camera Sensor ECU	Processes the images provided by the camera and runs computer vision algorithms to locate the position of the vehicle with in the lane
Car Display	Informs the driver about the status of the Lane Assistance System
Car Display ECU	Processes the incoming signals from the Power Steering ECU and the Camera ECU and signals the Car Display to show the appropriate status indicators
Driver Steering Torque Sensor	Measures the torque that is applied to the steering wheel
Electronic Power Steering ECU	Calculates how much torque shall be send to the Motor in order to implement the Lane Assistance functionality
Motor	Provides the torque requested from the Electronic Steering ECU 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 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 oscillating torque amplitude is below Max_Torque_Amplitude	C	50 msec	LDW vibration torque amplitude less than Max_Torque_Amplitude
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_torque_Frequency	C	50 msec	LDW vibration torque frequency less than Max_Torque_Frequency

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	Validate that drivers actually react to Max_Torque_Amplitude and can still control the vehicle	Verify that when the torque amplitude is greater than Max_Torque_Amplitude, the lane assistance output is set to zero within the 50 ms fault tolerant time interval

Functional Safety Requirement 01-02	Validate that drivers actually react to Max_Torque_Frequency and can still control the vehicle	Verify that when the torque frequency is greater than Max_Torque_Frequency, 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 msec	LKA torque equals zero

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	Validate with actual drivers that the max_duration did dissuade them from taking their hands off the wheel as they would in a self driving car	Verify that the system turns off if the lane keeping assistance exceeds max_duration.

Refinement of the System Architecture

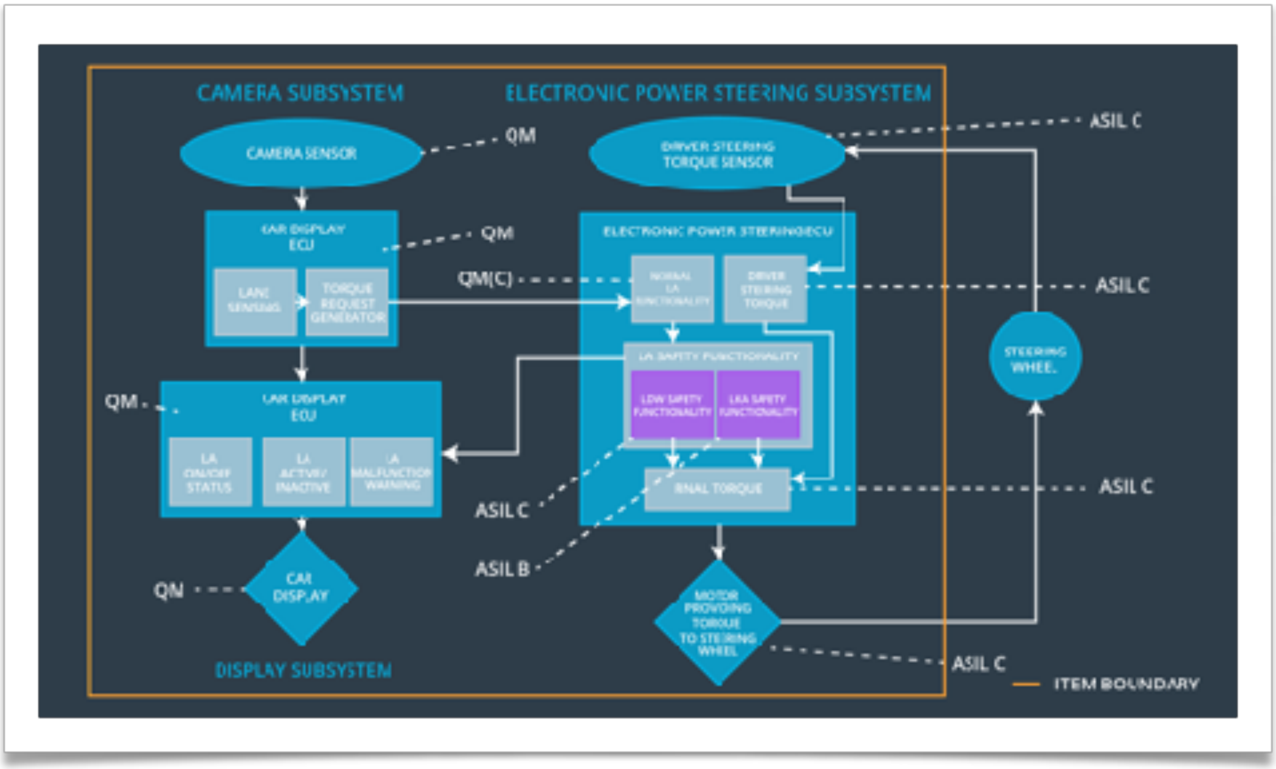

FIGURE 2. LANE ASSISTANCE SYSTEM REFINED ARCHITECTURE

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 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

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the Lane Departure Warning	Malfunction_01 Malfunction_02	Yes	Turn on Lane Assistant malfunction warning light
WDC-02	Turn off the Lane Keeping Assistant	Malfunction_03	Yes	Turn on Lane Assistant malfunction warning light