Functional Safety Concept Lane Assistance

Document Version: [Version]
Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description

5/24/2018	V1	Shamsher Singh Thind	Version-1

Table of Contents

Purpose of the Functional Safety Concept

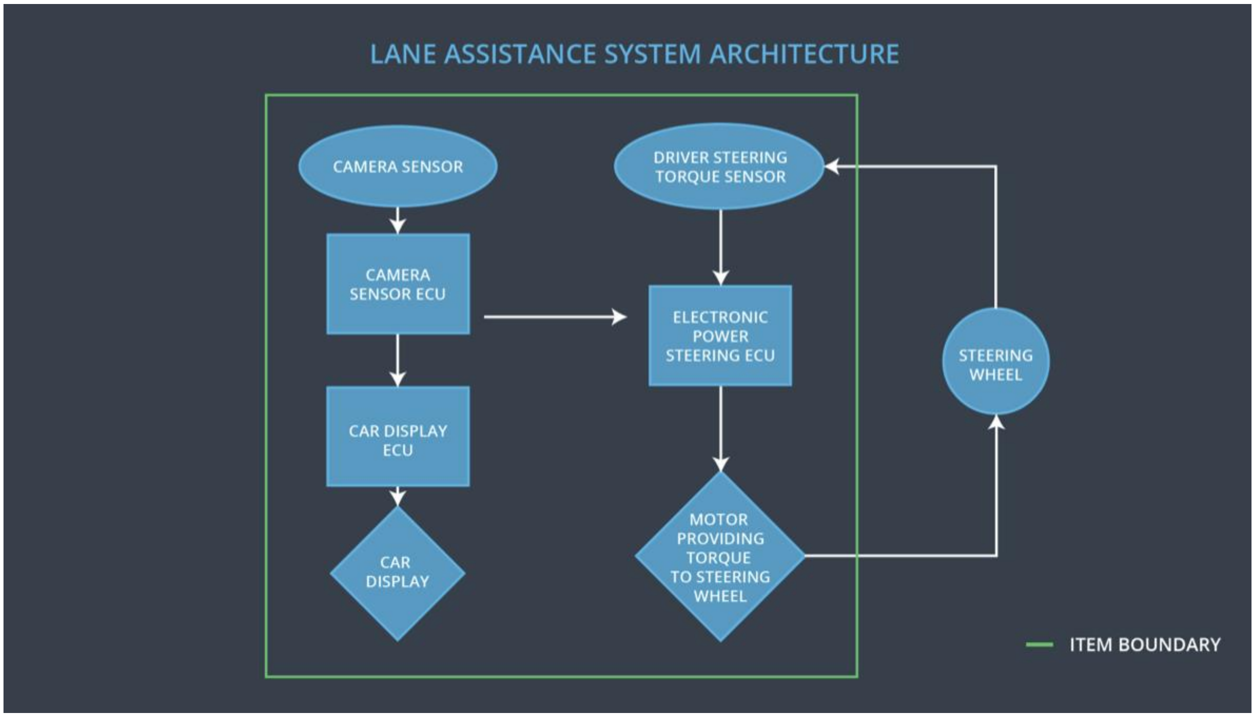
The functional safety concept is to document the general functionality of the item without going into technical detail. This document also identifies safety requirements and then allocate those requirements to different parts of the item architecture. Functional safety requirements also have attributes that are specified in the functional safety concept. Further to prove that a system actually meets requirements, they have to be verified and validated.

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 that 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

Description of architecture elements

Element	Description

Camera Sensor	It reads in images from the road and sends to camera sensor ECU
Camera Sensor ECU	Identifies when the vehicle has accidentally departed its lane, and sends the appropriate message to the car display ECU and electronic power steering ECU
Car Display	It displays the actual output generated by car display ECU
Car Display ECU	It generates output for LA on/off status, LA Active/inactive, LA malfunction warning
Driver Steering Torque Sensor	It reads the steering torque on the steering wheel
Electronic Power Steering ECU	It reads data from Steering Torque Sensor and Torque request generator and generates final torque signal to motor
Motor	It actuates the final torque provided by 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	MORE	The lane departure warning function applies an oscillating torque with very high torque amplitude (above limit)

	feedback		
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

[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	50 ms	Set Vibration to zero when fault detected
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 ms	Set Vibration to zero when fault detected

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

ID	**Validation Acceptance Criteria and Method**	**Verification Acceptance Criteria and Method**
Functional	validate how drivers react to different	verify that the torque amplitude

Safety Requirement 01-01	torque amplitudes	crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval
Functional Safety Requirement 01-02	validate how drivers react to different torque frequencies	verify that the torque frequencies crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval

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

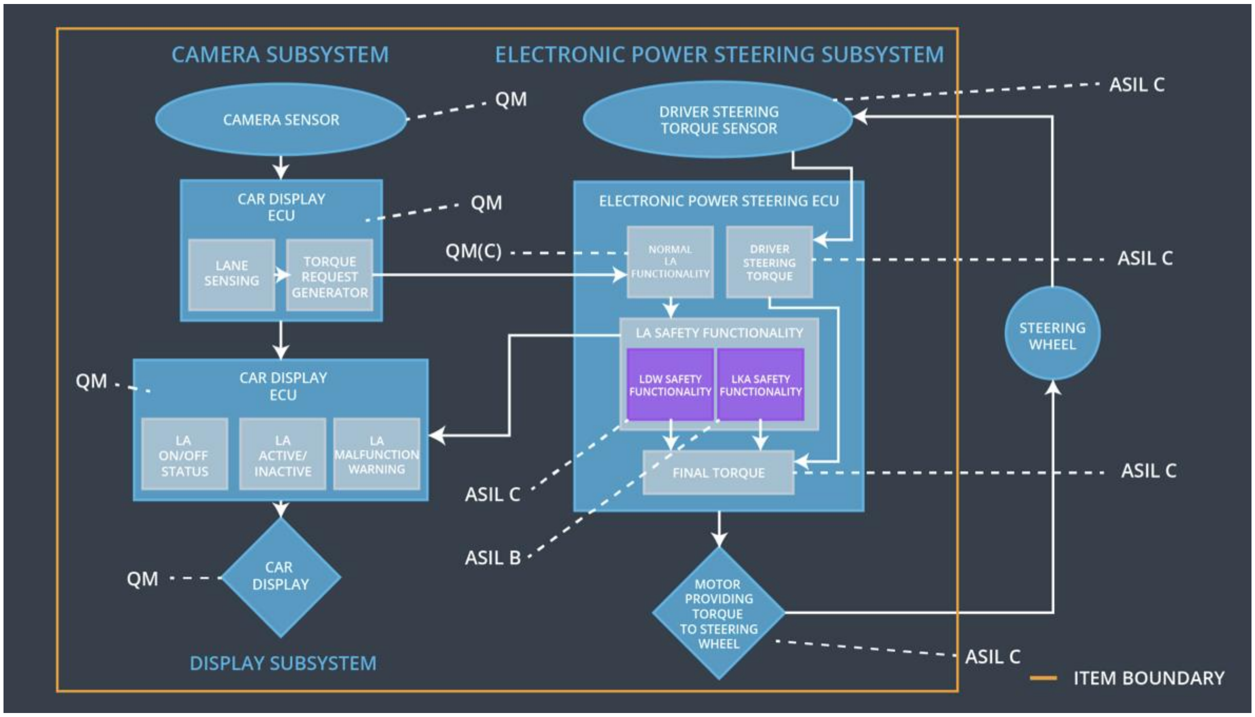
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500 ms	Reduce the torque by lane keeping system to zero when fault detected

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 that the max_duration chosen really did dissuade drivers from taking their hands off the wheel	Verify that the system really does turn off if the lane keeping assistance every exceeded max_duration

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 oscillating torque amplitude is below Max_Torque_Amplitude	Responsible	Not responsible	Not responsible
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	Responsible	Not responsible	Not responsible
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	Responsible	Not responsible	Not responsible

Warning and Degradation Concept

ID	**Degradation Mode**	**Trigger for Degradation Mode**	**Safe State invoked?**	**Driver Warning**
WDC-01	Lane Departure warning functionality is set to zero	Malfunction_01 Malfunction_02	Yes	Malfunction warning on with Lane Departure warning indicator signal
WDC-02	Lane keeping assistance functionality is set to zero	Malfunction_03	Yes	Malfunction warning on with Lane keeping assistance indicator signal