Functional Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
01.03.2018	1.0	Qingqing Xia	First version of this document

Table of Contents

Purpose of the Functional Safety Concept

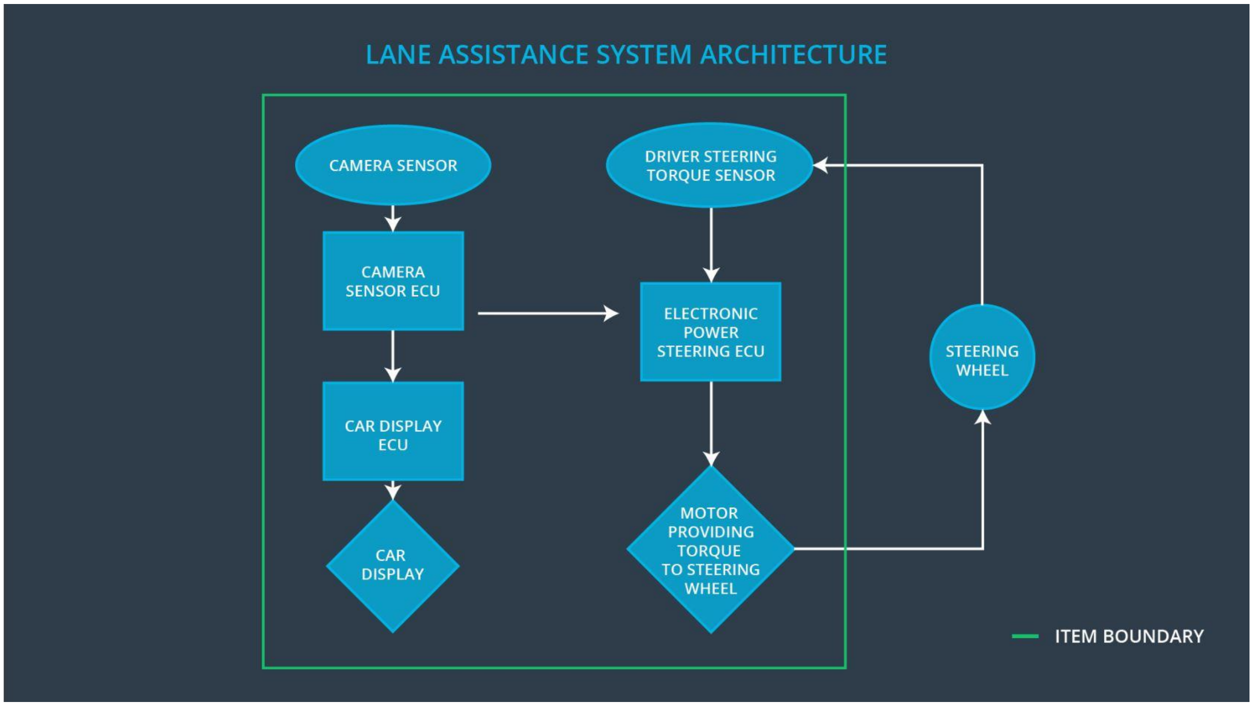
Functional safety concept is looking at the item from a higher level. It looks at the general functionality of the item. In the technical safety concept, it will start looking at different parts of the items, like sensors, control units and actuators. The functional safety concept and technical safety concept are similar in that one will need to identify new requirements and allocate these requirements to system diagrams.

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 the driver cannot misuse the system for autonomous driving.

Preliminary Architecture


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

Description of architecture elements

Element	Description
Camera Sensor	Deliver road images to the Camera Sensor ECU.

Camera Sensor ECU	Detects lane lines and determines when the vehicle leaves the lane by mistake. Generates a torque request to the Electronic Power Steering ECU. Triggering the Car Display ECU.
Car Display	Show warning to the driver
Car Display ECU	Generates warning signals triggered by input from Camera Sensor ECU and Electronic Power Steering ECU.
Driver Steering Torque Sensor	Measure the steering torque by the driver and provides it to Electronic Power Steering ECU.
Electronic Power Steering ECU	Receives the torque by the driver from Driver Steering Torque Sensor and calculates the amount of torque based on Camera Sensor ECU request
Motor	Receives torque calculated by Electronic Power Steering ECU and applies it to 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
Malfunction_04	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	NO	The camera can’t detect the lanes, which lead to uncertain behavior of the LKA.

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	Vibration torque amplitude below 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	50ms	Vibration frequency is below 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	To prove we have chosen a Max_Torque_Amplitude reasonable value. We could test how drivers react to different amplitude frequencies to prove that we chose an appropriate value.	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	To prove we have chosen a reasonable Max_Torque_Frequency value. We could test how drivers react to different torque frequencies to prove that we chose an appropriate value.	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:

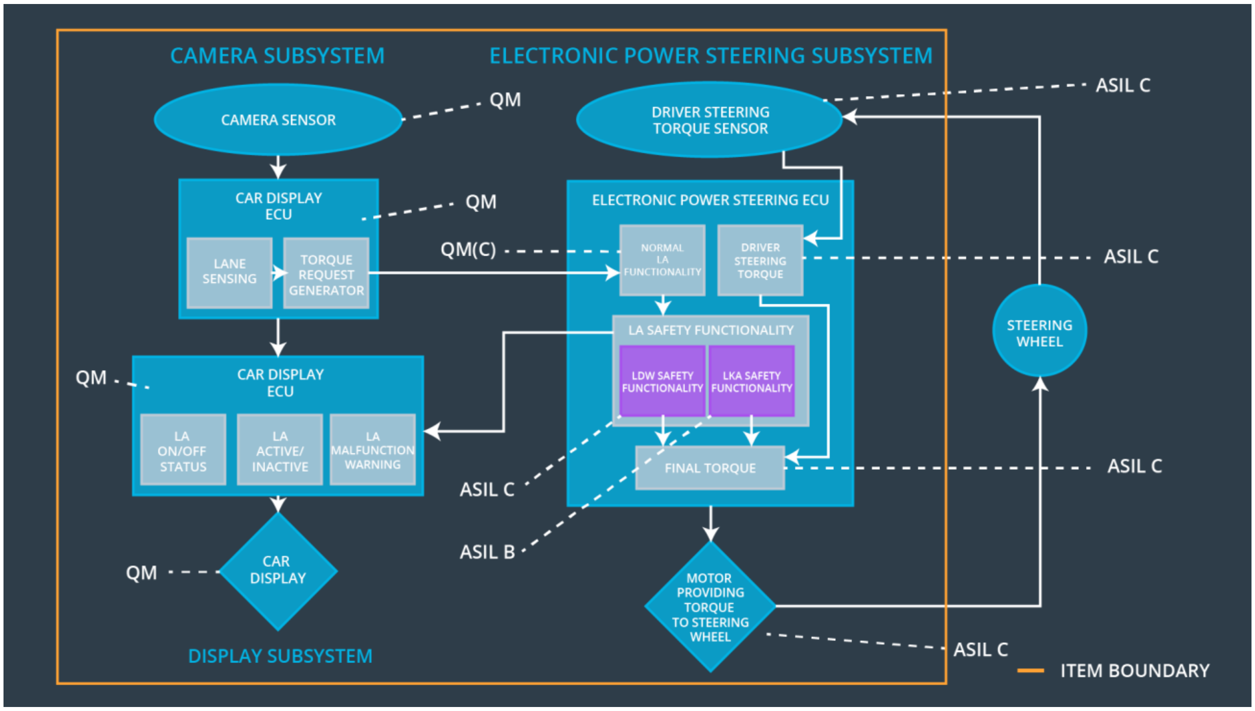
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only Max_Duration.	B	500ms	Lane Keeping Assistance torque is zero.
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that lane keeping assistance torque zero if camera sensor ECU states Lane_Not_Found is true	C	50ms	Deactive the function

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

Functional Safety Requirement 02-02	Validate the Lane Keeping assistance shall be deactivated when the camera sensor can’t detect the lane correctly any more.	Verify the system does deactivate the Lane Keeping Assistance if the camera sensor can’t (correctly) detector lanes any more.

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 Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	x		
Functional	The Lane Departure Warning	x		

Safety Requirement 01-02	item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.			
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane that the Lane Keeping Assistance torque is applied only Max_Duration.	**x**		
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that lane keeping assistance torqueis zero if camera sensor ECU states Lane_Not_Found is true	**x**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off Lane Departure Warning functionality	Malfunction_01, Malfunction_02,	Yes	Lane Departure Warning Malfunction Warning on Car Display
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03	Yes	Lane Keeping Assistance Malfunction Warning on Car Display