Functional Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
2018-01-26	1.0	Josef Steinbaeck	First attempt

Table of Contents

Purpose of the Functional Safety Concept

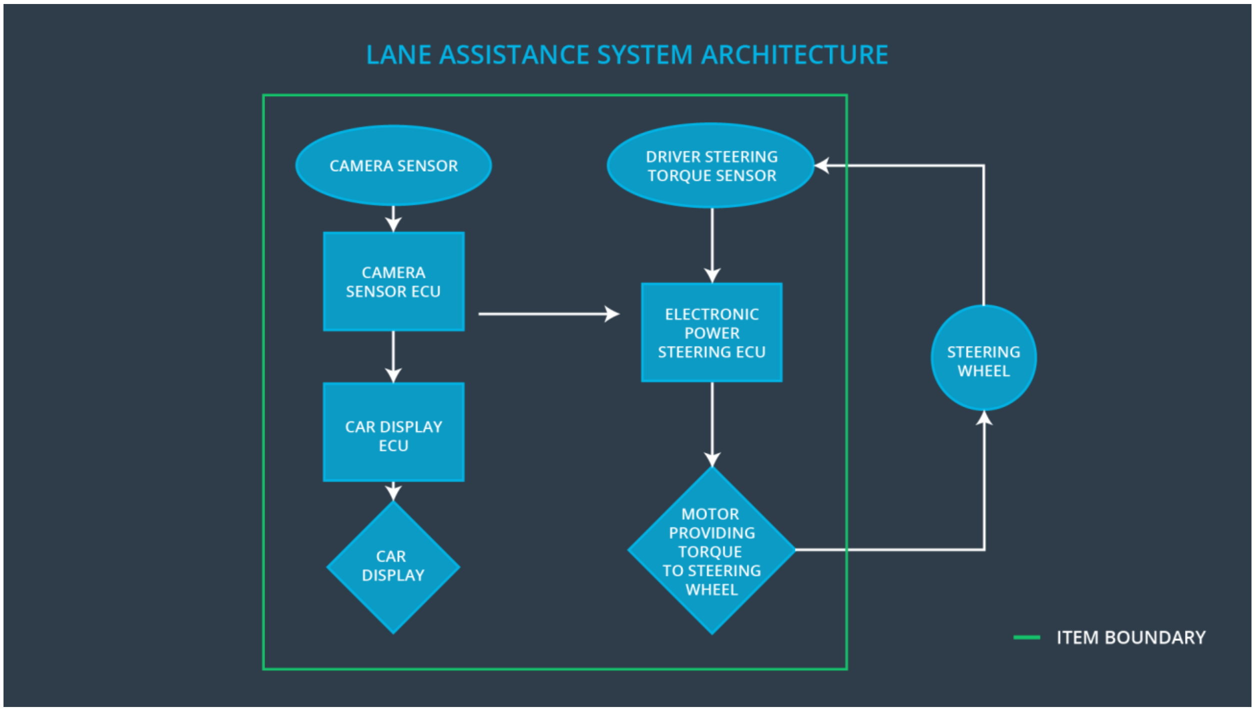
Identify new requirements and allocate these requirements to system diagrams. The functional safety concept does not go into technical details. It looks at the generals functionality of the item.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscillating torque to the steering wheel from the lane departure warning function shall be limited
Safety_Goal_02	The lane keeping assistance functionality shall be time limited

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	The camera sensor reads in images from the road
Camera Sensor ECU	Identifies when the vehicle has accidentally departed the lane and sends the appropriate messages to the Car Display ECU and the Electronic Power Steering ECU
Car Display	The display contains lights indicating the current state of the lane assistance system.
Car Display ECU	Controls a light that tells the driver if the lane keeping item is on or off. And a second control that tells the driver if the lane departure warning is activated or not.
Driver Steering Torque Sensor	Senses the steering torque applied by the driver and sends it to the Electronic Power Steering ECU.
Electronic Power Steering ECU	Combines the vibrational torque request from the Camera ECU and the driver steering torque from the Driver Steering Torque Sensor in order to generate a final electronic power steering torque output to the Motor.
Motor	Moves 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 ms	The torque request from the lane keeping assistance will be set to zero
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	The torque request from the lane keeping assistance will be set to zero

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 how drivers react to different torque amplitude and frequencies to prove that we chose an appropriate value	When the torque amplitdue crosses the limit the lance assitance output is set to zero within 50 ms (e.g. software test inserting a fault)
Functional Safety Requirement 01-02	Test how drivers react to different torque amplitude and frequencies to prove that we chose an appropriate value	When the torque amplitdue crosses the limit the lance assitance output is set to zero within 50 ms (e.g. software test inserting a fault)

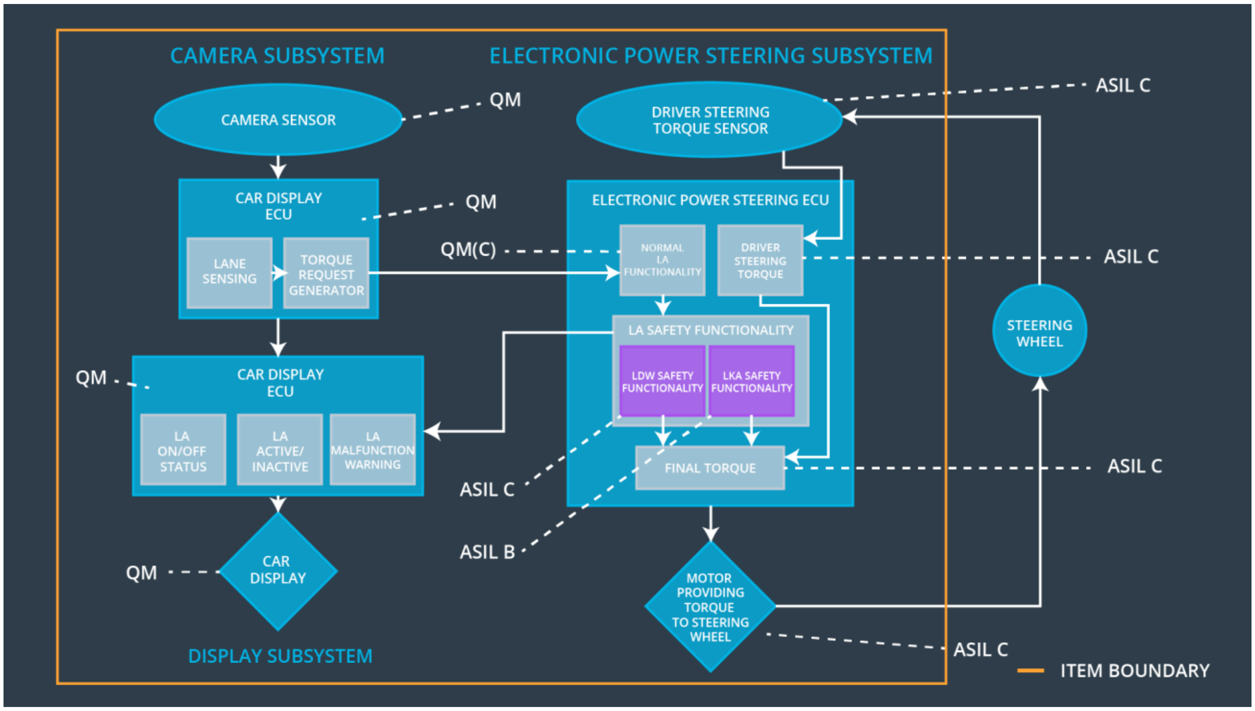
Lane Keeping Assistance (LKA) Requirements:

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	The torque request from the lane keeping assistance will be set to 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	Test and validate that the max_duration really did dissuade drivers from taking their hands off the wheel.	Verify that system really does turn off its 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	X		
Functional Safety Requirement 01-02	The lane keeping item 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 functionality	lane departure oscillating torque frequency or amplitude too high	Yes	Warning light on the dashboard
WDC-02	Turn off functionality	lane keeping assistance torque is applied for Max_Time	Yes	Warning light on the dashboard