Functional Safety Concept Lane Assistance

Document Version: 1.3

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
06/23/19	1.0	Adam Gotlib	First draft
06/23/19	1.1	Adam Gotlib	Added explanation of document purpose
06/23/19	1.2	Adam Gotlib	Replaced refined architecture diagram
06/23/19	1.3	Adam Gotlib	Removed template-specific parts of the document

Table of Contents

Purpose of the Functional Safety Concept

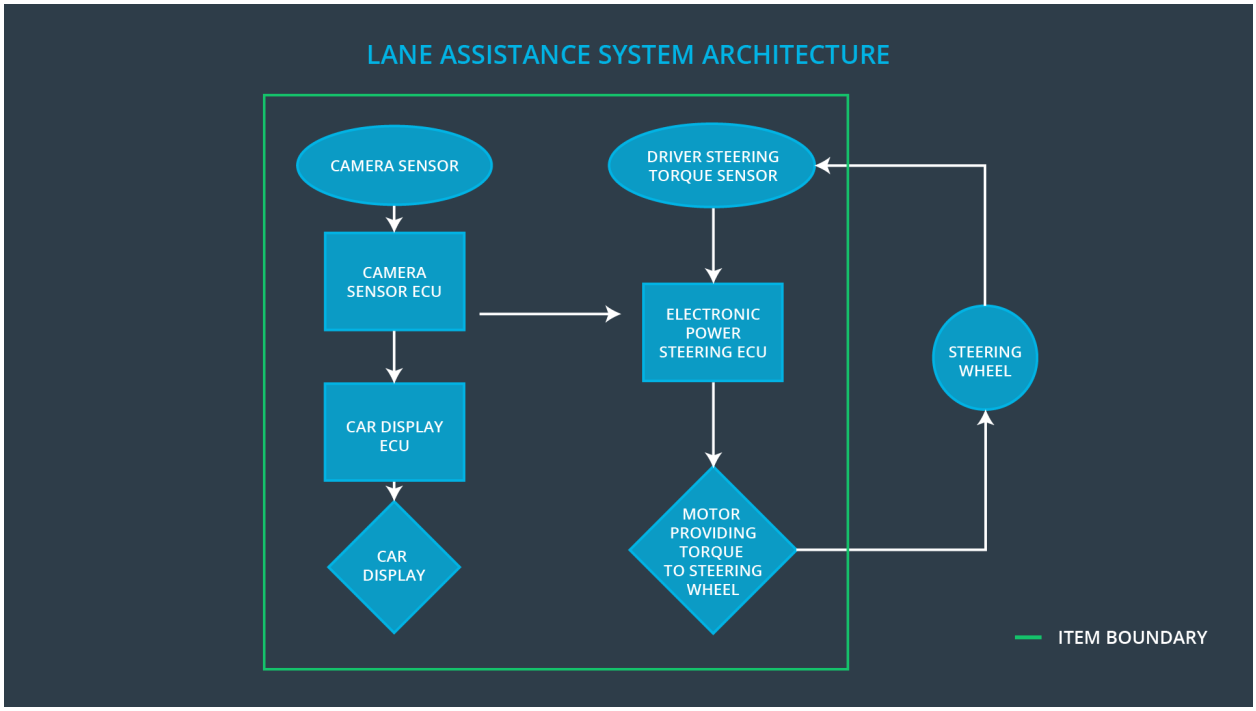
The Functional Safety Concept serves the purpose of refining Safety Goals into Functional Safety Requirements and allocating them to appropriate places in the item architecture.

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 LDW function shall be limited.
Safety_Goal_02	The 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.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Captures images in front of the vehicle.
Camera Sensor ECU	Analyses captured images and determines when the vehicle leaves the lane by mistake.
Car Display	Displays visual cues for the driver, informing them of functioning of the system.
Car Display ECU	Controls the Car Display based on inputs from other elements.
Driver Steering Torque Sensor	Measures the torque provided by the driver.
Electronic Power Steering ECU	Estimates the required amount of additional torque to be applied based on a lane assistance system torque request and the torque provided by the driver.
Motor	Applies additional torque 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 ms	The LDW function shall deactivate and display a visual warning to the driver.
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 LDW function shall deactivate and display a visual warning to the driver.

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	The Max_Torque_Amplitude value shall be validated to be below acceptable level for most of the drivers.	The LDW function shall be verified to deactivate and display a visual warning to the driver within 50ms if the oscillating torque amplitude is above Max_Torque_Amplitude.
Functional Safety Requirement 01-02	The Max_Torque_Frequency value shall be validated to be below acceptable level for most of the drivers.	The LDW function shall be verified to deactivate and display a visual warning to the driver within 50ms if the oscillating torque frequency is above Max_Torque_Frequency.

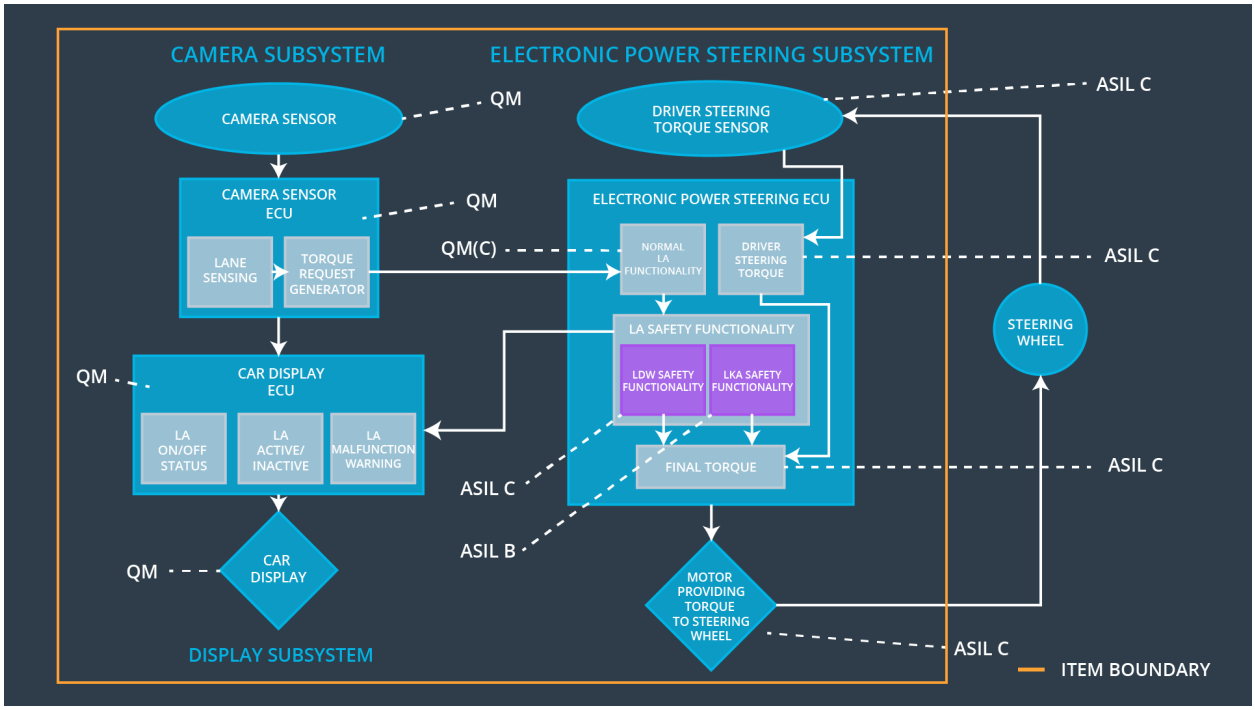
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied only for Max_Duratoin.	B	500 ms	The LKA function shall deactivate and display a visual warning to the driver.

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 value shall be validated to be shorter than time needed for a driver to lose attention.	The LKA function shall be verified to deactivate and display a visual warning to the driver within 500ms if the lane keeping assistance torque is applied for more than Max_Duratoin.

Refinement of the System Architecture


CAMERA SUBSYSTEM
ELECTRONIC POWER STEERING SUBSYSTEM
CAMERA SENSOR
QM
DRIVER STEERING TORQUE SENSOR
ASIL C
CAMERA SENSOR ECU
QM
ELECTRONIC POWER STEERING ECU
LANE SENSING
TORQUE REQUEST GENERATOR
QM(C)
NORMAL LA FUNCTIONALITY
DRIVER STEERING TORQUE
ASIL C
STEERING WHEEL
LA SAFETY FUNCTIONALITY
LDW SAFETY FUNCTIONALITY
LKA SAFETY FUNCTIONALITY
QM
CAR DISPLAY ECU
LA ON/OFF STATUS
LA ACTIVE/ INACTIVE
LA MALFUNCTION WARNING
FINAL TORQUE
ASIL C
ASIL C
ASIL B
QM
CAR DISPLAY
MOTOR PROVIDING TORQUE TO STEERING WHEEL
ASIL C
DISPLAY SUBSYSTEM
ITEM BOUNDARY

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.	**YES**	**NO**	**NO**
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	**YES**	**NO**	**NO**
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied only for Max_Duratoin.	**YES**	**NO**	**NO**

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Deactivate LDW function.	Malfunction_01 Malfunction_02	YES	Visual display
WDC-02	Deactivate LKA function.	Malfunction_03	YES	Visual display