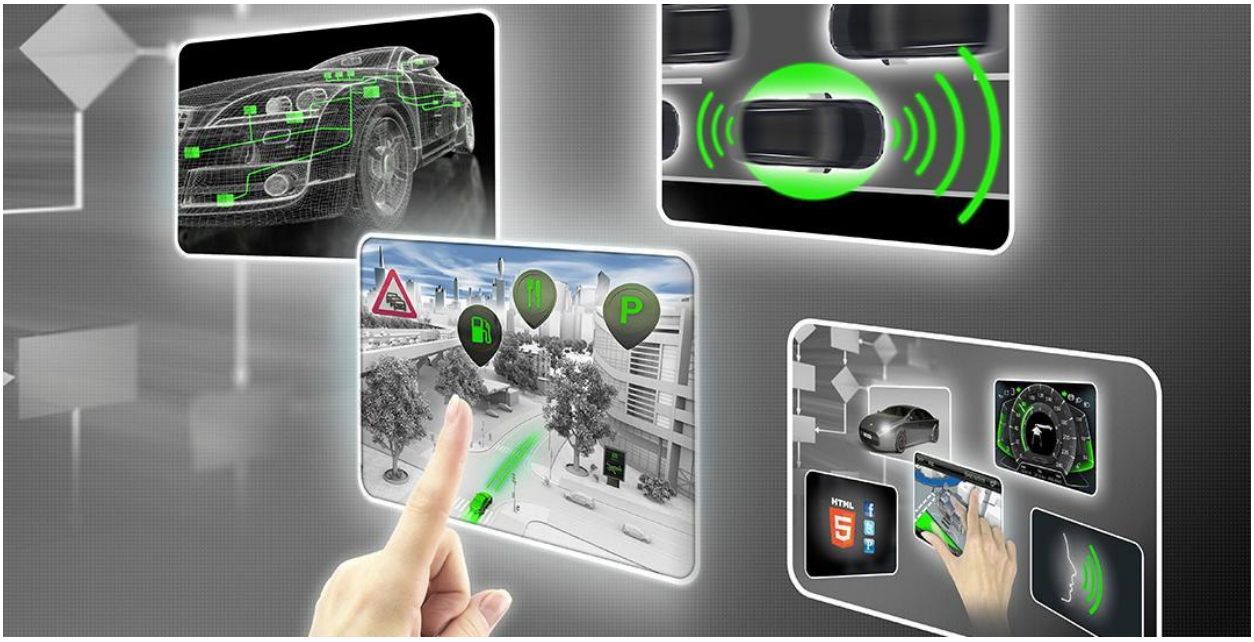


Functional Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
12/22/2018	1.0	Luis Güette	First Version

Table of Contents

Purpose of the Functional Safety Concept

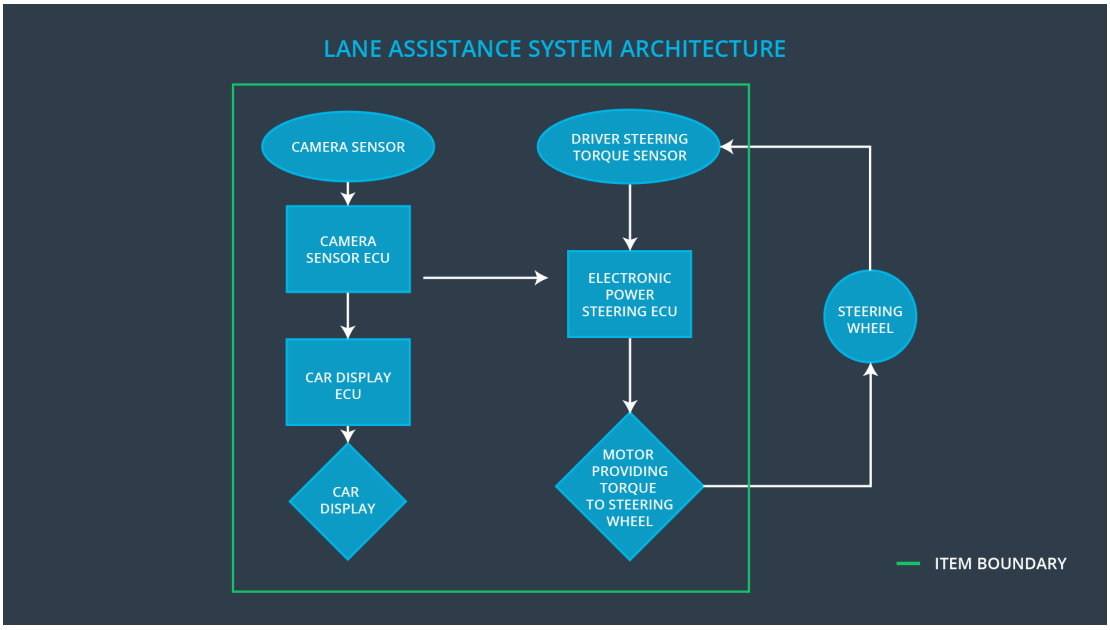
In the functional safety concept, the functional safety requirements are defined, which are allocated in the relevant parts of the system diagram.

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
Safety_Goal_03	The Lane Departure Warning function shall be deactivated when the camera sensor stop working.
Safety_Goal_04	The Lane Keeping Assistance function shall be deactivated when the camera sensor stop working.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Gets images from the road and sends them to the ECU
Camera Sensor ECU	Calculate the vehicle position relative to the lane
Car Display	Give a feedback to the driver about vehicle LAS status and warnings
Car Display ECU	Receive data from the Camera Sensor ECU, analyze it, sends it to the Car Display, and sends the necessary torque, if needed, to the Electronic Power Steering ECU
Driver Steering Torque Sensor	Sense the torque applied by the driver
Electronic Power Steering ECU	Gets torque data from the Driver Steering Torque Sensor and the Camera Sensor ECU, analyze it, and request the necessary torque to be applied by the motor.
Motor	Applies the torque requested by the 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

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 LDW 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 LDW 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	Lane Keeping function is always activated which can be misused by the driver as a self-driving car function
Malfunction_04	The Lane Departure Warning function shall be deactivated when the camera sensor stop working.	WRONG	The camera sensor stop working and the Lane Departure Warning function continue to be activated.
Malfunction_05	The Lane Departure Warning function shall be deactivated when the camera sensor stop working.	WRONG	The camera sensor stop working and the Lane Keeping Assistance function continue to be activated.

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 Departure Warning 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 Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50ms	Vibration frequency is below Max_Torque_Frequency.
Functional Safety Requirement 01-03	The Lane Departure Warning function shall be deactivated when the camera sensor stop working.	C	50ms	Function is deactivated

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 Max_Torque_Amplitude is enough to be detected by a driver and not to cause loss of steering.	Verify that the LAS turn off if Max_Torque_Amplitude is exceeded
Functional Safety Requirement 01-02	Validate Max_Torque_Frequency is enough to be detected by a driver and not to cause loss of steering.	Verify that the LAS turn off if Max_Torque_Frequency is exceeded
Functional Safety Requirement 01-03	Validate LAS is turned off if the camera sensor is not working	Verify that the LAS turn off if the camera is not working

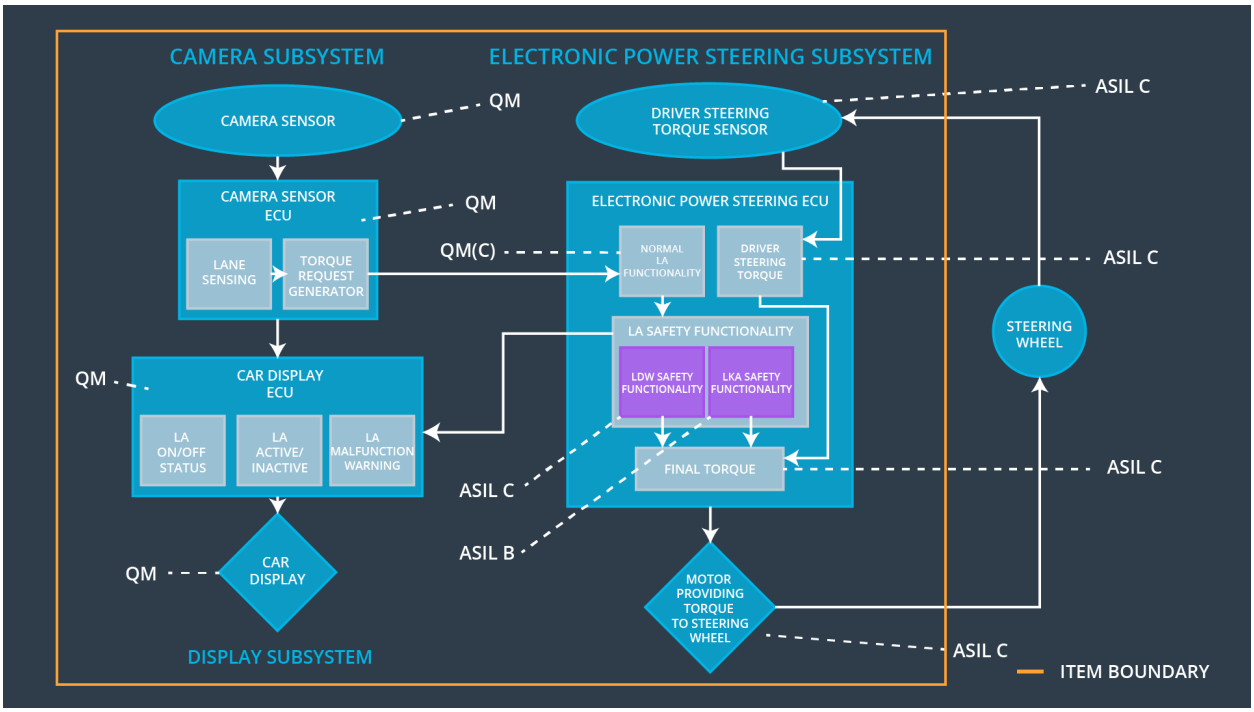
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The Lane Keeping Assistance function shall be time limited, and additional steering torque shall end after a Max_Duration interval so the driver cannot misuse the system for autonomous driving	B	500ms	LKS is turned of after a Max_Duration interval
Functional Safety Requirement 02-02	The Lane Keeping Assistance function shall be deactivated when the camera sensor stop working.	C	50ms	Function is deactivated

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 Max_Duration is enough, so the driver cannot use the function as a self-driving car	Verify that the LKS is deactivated after Max_Duration interval
Functional Safety Requirement 02-02	Validate that the LKA system shall deactivate when camera sensor is not working	Verify that the LKA system deactivates when camera sensor is not working

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 Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	**X**		

Functional Safety Requirement 01-03	The Lane Departure Warning function shall be deactivated when the camera sensor stop working.	**X**		
Functional Safety Requirement 02-01	The Lane Keeping Assistance function shall be time limited, and additional steering torque shall end after a Max_Duration interval so the driver cannot misuse the system for autonomous driving	**X**		
Functional Safety Requirement 02-02	The Lane Keeping Assistance function shall be deactivated when the camera sensor stop working.	**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, Malfunction_04	yes	LDW malfunction warning on Car Display
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03, Malfunction_05	yes	LKA malfunction warning on Car Display