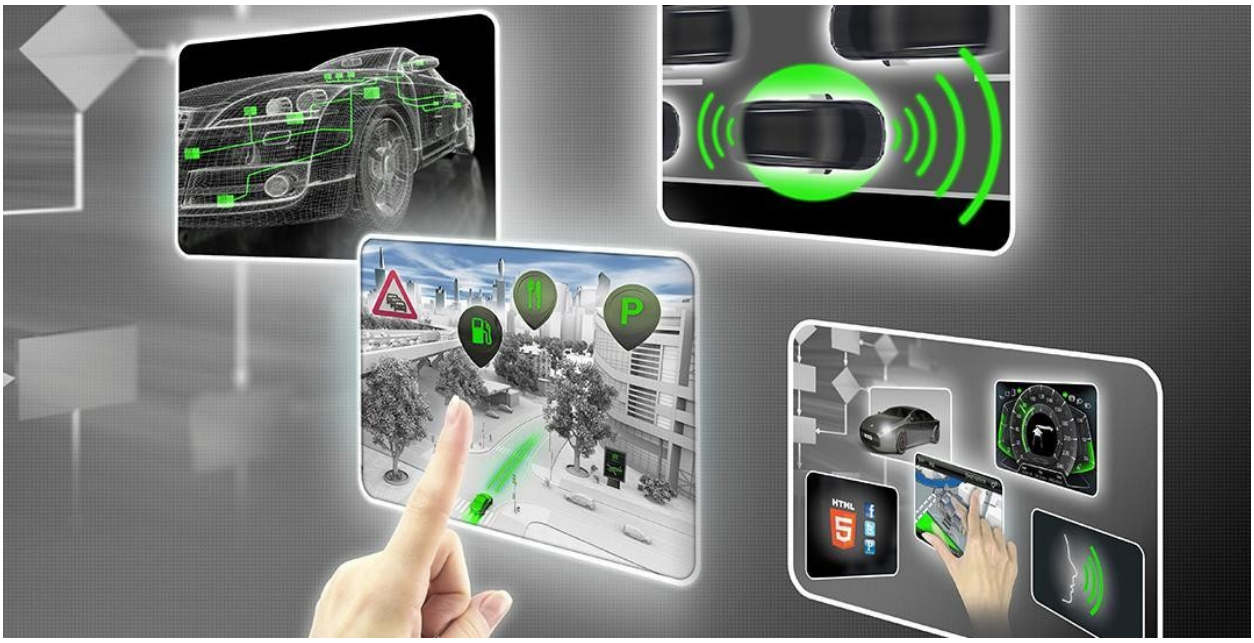
Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
3/21/18	1.0	David G	First draft

Table of Contents

Purpose of the Functional Safety Concept

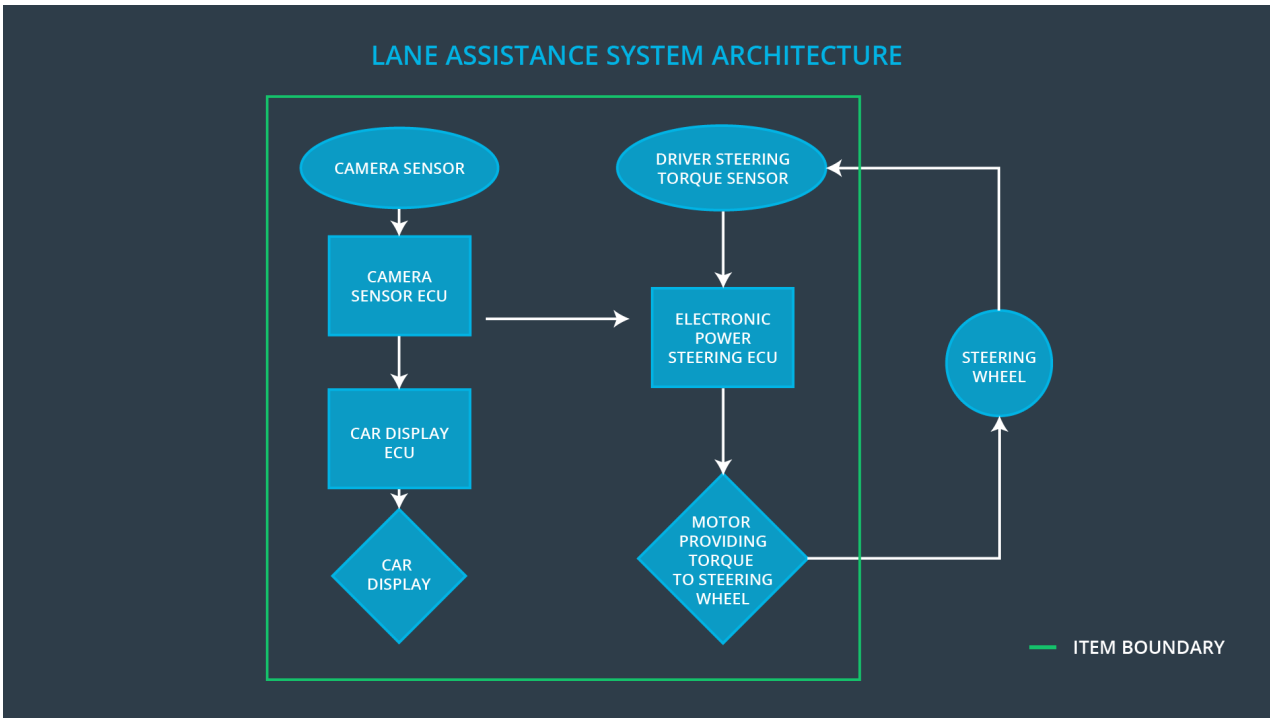
A functional safety concept is a high-level evaluation of safety requirements and how they fit into the preliminary architecture of the system. Each safety requirement is also evaluated and attributed an ASIL, fault tolerant time interval, and safe state. A functional safety concept also includes verification and validation of the system to prove that the system meets requirements.

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	Lane keeping assistance function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver can not misuse the system for autonomous driving.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Visual observation of driving surface for lane detection. Signal sent to camera sensor ecu.
Camera Sensor ECU	Lane sensing and torque request generator. Signal sent to electronic power steering ecu.
Car Display	Visual display to driver of LDW/LKA status from car display ecu.
Car Display ECU	From camera sensor ecu, receives LDW and LKA on/off status, active/inactive status, malfunction warning.
Driver Steering Torque Sensor	Measures driver torque input. Sends input to electronic power steering ecu.
Electronic Power Steering ECU	Recieves torque request from camera sensor ECU and driver torque sensor and computes amount of torque to request from the motor.

Motor	Recieves torque request from electronic power steering ecu and applies 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.

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	LDW function turned off.
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	LDW function turned off.

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 driver reaction to different torque amplitudes to validate an appropriate value was chosen.	Verify that the LDW function turns off when the torque amplitude crosses the limit, and the lane assistance output is set to zero within the 50 ms fault tolerant time interval.
Functional Safety Requirement 01-02	Test driver reaction to different torque frequencies to validate an appropriate value was chosen.	Verify that the LDW function turns off when the torque frequency crosses the limit, and the lane assistance output is set to zero within the 50 ms fault tolerant time interval.

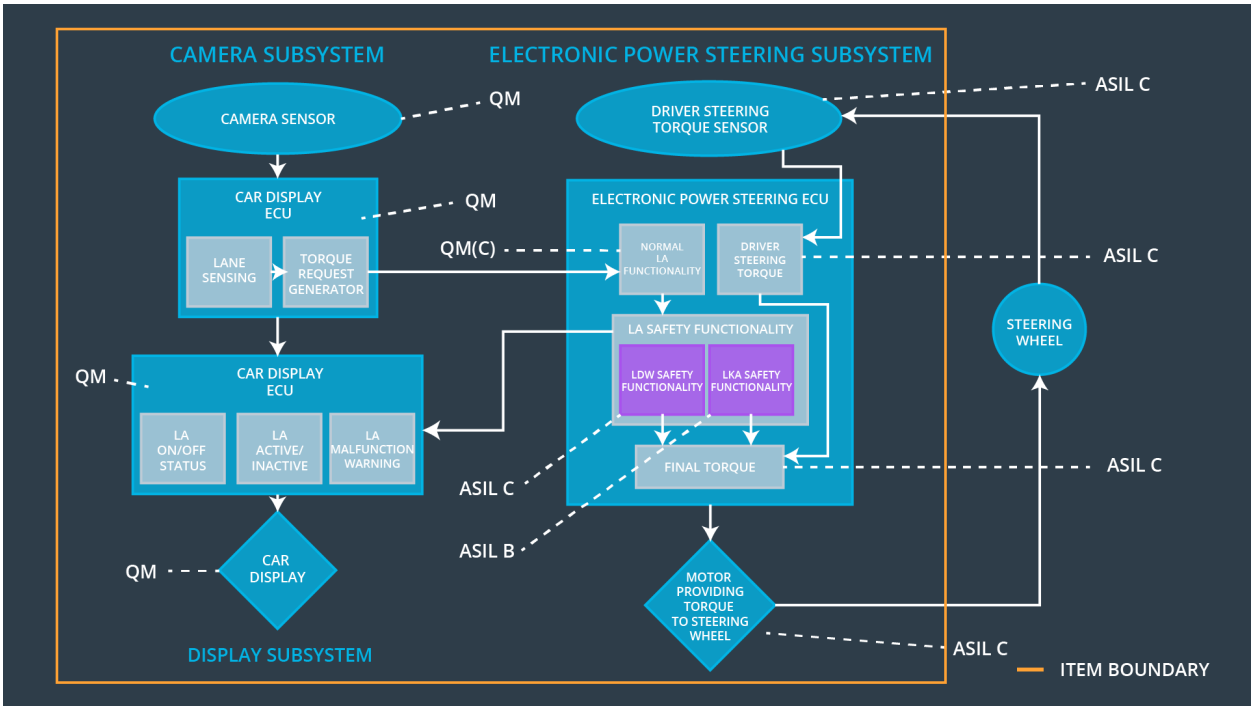
Lane Keeping Assistance (LKA) Requirements:

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 for only Max_Duration.	B	500 ms	LKA function turned off.

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 dissuades drivers from taking their hands off the wheel.	Verify that the LKA function turns off if the lane keeping assistance exceeds 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 LDW function.	Malfunction_01 / Malfunction_02	Yes	Malfunction warning on Car Display.
WDC-02	Turn off LKA function.	Malfunction_03	Yes	Malfunction warning on Car Display.