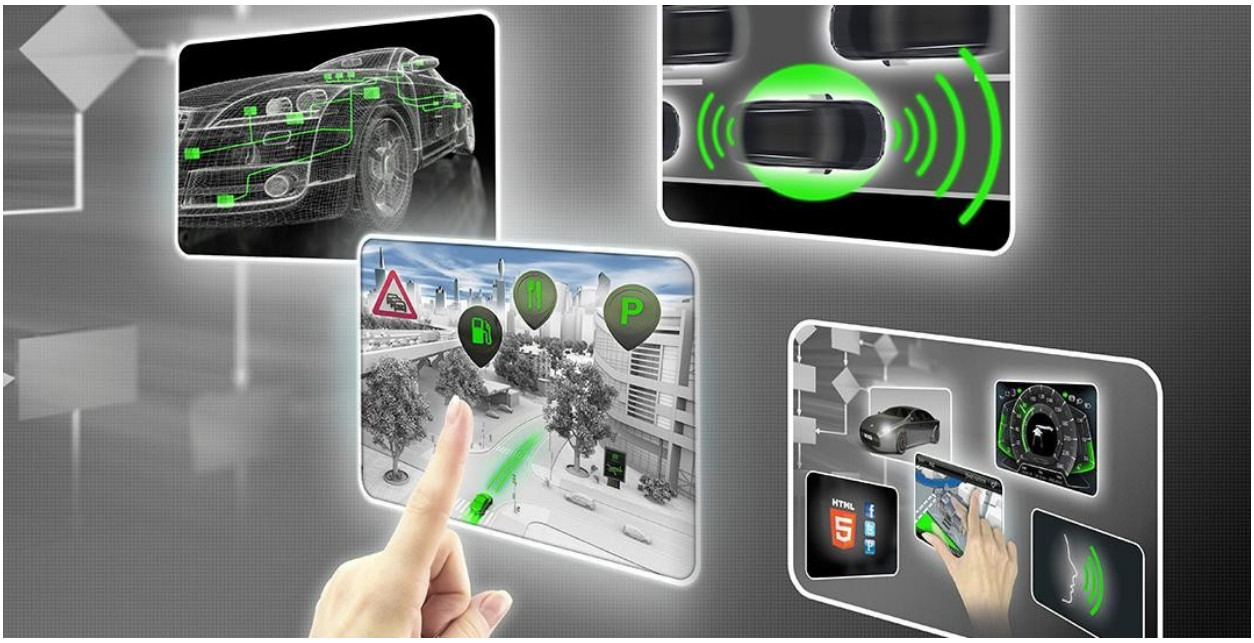
Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
2018-06-12	1.0	Markus Isaksson	First attempt

Table of Contents

Purpose of the Functional Safety Concept

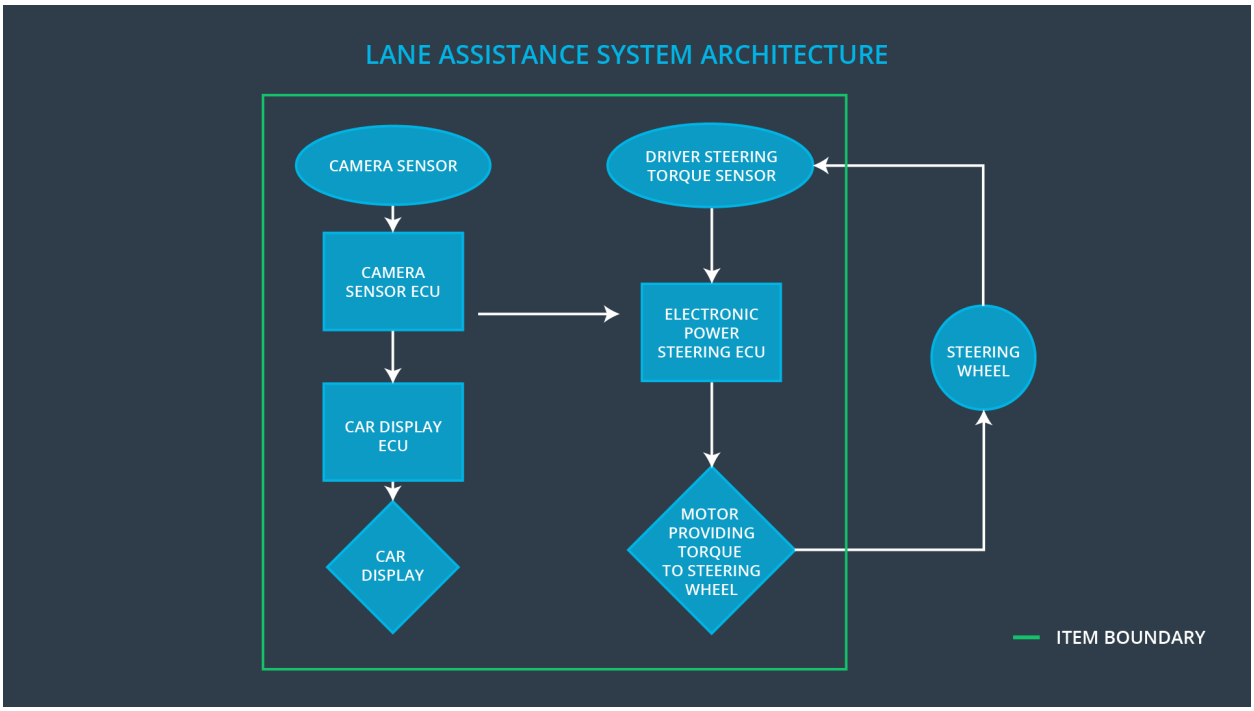
The functional safety concept refines the Safety Goals from the Hazards Analysis and Risk Assessment into functional safety requirements. These requirements are then allocated to relevant parts of the system architecture. The allocation might involve expanding the system architecture with new element blocks.

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 the additional steering torque shall end after a given time interval so that the driver cannot misuse the system for autonomous driving.
Safety_Goal_03	The steering torque from the lane keeping assistance function shall be limited.
Safety_Goal_04	The lane keeping assistance function shall not interfere when the torque applied on the steering wheel by the driver suggests that the lane change is intentional.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Forward looking camera capturing images of the road ahead of ego vehicle.
Camera Sensor ECU	Detecting lane lines in the Camera Sensor images and determines when the vehicle leaves the lane by mistake. Implements the Lane Departure Warning and Lane Keeping Assistance functions. Sends messages to the Electronic Power Steering ECU requesting torque input on the steering wheel. Sends status messages to the Car Display ECU.
Car Display	Display mounted in the vehicle dashboard to present information to the driver.
Car Display ECU	Create the images displayed on the Car Display. The status messages from the Camera Sensor ECU is shown as symbols and/or text.
Driver Steering Torque Sensor	Measures the torque applied on the steering wheel by the driver.
Electronic Power Steering ECU	Controls the torque applied on the steering wheel by this item.

Motor	Steering wheel torque actuator.

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	The lane departure warning is giving **MORE** torque than what is safe	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	The lane departure warning is giving **MORE** torque than what is safe	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	The lane keeping assistance has **NO** time limit	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	The lane keeping assistance is giving **MORE** torque than what is safe	The lane keeping assistance function applies a very high torque (above limit)

Malfunction_05	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	The lane keeping assistance has **NO** input from the driver steering torque sensor	The lane keeping assistance function does not consider driver steering torque when deciding if a lane change is intentional.

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 electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Lane Assistance is turned off
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	Lane Assistance is 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	Validate that the Max_Torque_Amplitude not is too high to affect the controllability of the vehicle, still adequate to be clearly noticed by the driver.	Verify by fault injection in the Camera Sensor ECU and measure that no torque is applied on the steering wheel after FTTI.
Functional Safety Requirement 01-02	Validate that the Max_Torque_Frequency not is too high to affect controllability of the vehicle, still adequate to be clearly noticed by the driver.	Verify by fault injection in the Camera Sensor ECU and measure that no torque is applied on the steering wheel after FTTI.

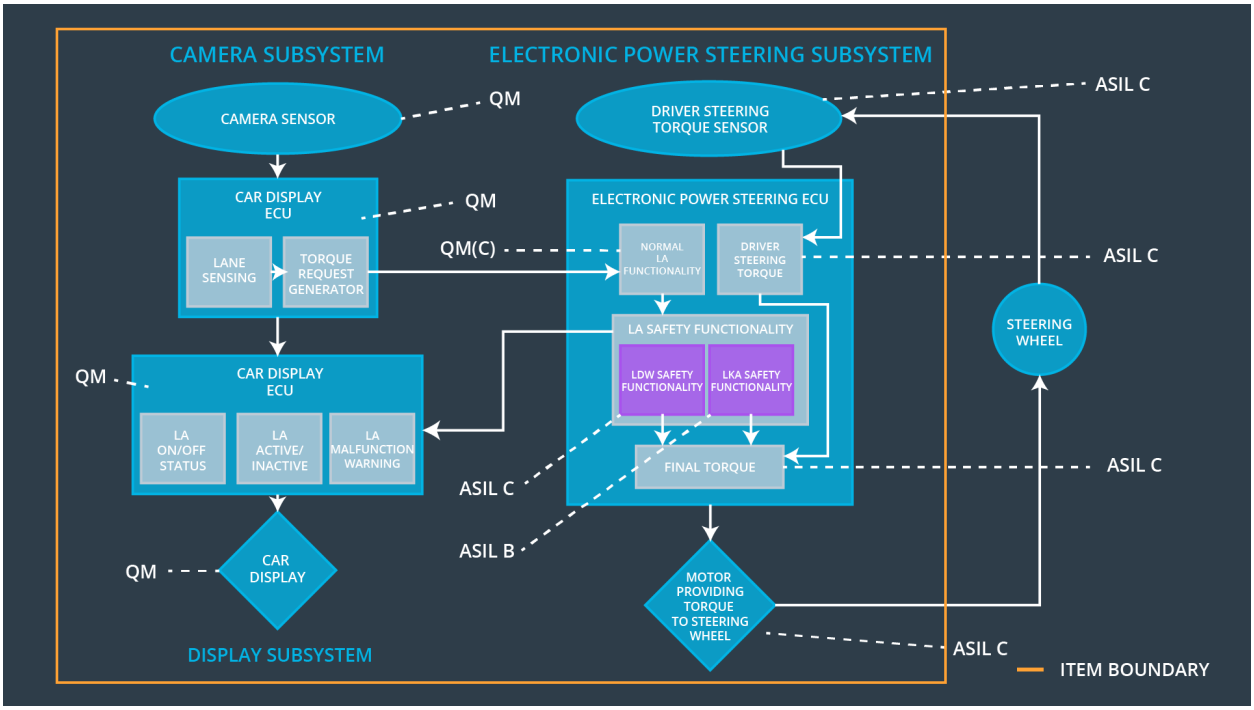
Lane Keeping Assistance (LKA) Requirements:

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 is deactivated
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that the lane keeping assistance torque is below Max_Lane_Keep_Torque.	B	50 ms	Lane Assistance is turned off
Functional Safety Requirement 02-03	The electronic power steering ECU shall ensure that the lane keeping assistance applies no torque when the driver steering torque exceeds Max_Drifting_Torque.	A	50 ms	LKA 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 the Max_Duration actually dissuades drivers from taking their hands off the wheel, still is adequate to correct unintentional lane changes.	Verify by fault injection in the Camera Sensor ECU and measure that no torque is applied on the steering wheel after Max_Duration + FTTI.
Functional Safety Requirement 02-02	Validate that the Max_Lane_Keep_Torque not is too high to affect the controllability of the vehicle, still adequate to correct the direction of the vehicle on curvy roads at high speed.	Verify by fault injection in the Camera Sensor ECU and measure that no torque is applied on the steering wheel after FTTI.
Functional Safety Requirement 02-03	Validate that Max_Drifting_Torque is less than typical steering torques applied by driver during collision avoidance.	Verify by applying a driver steering torque of Max_Drifting_Torque and by fault injection in the Camera Sensor ECU, then measure that this item applies no torque on the steering wheel after FTTI.

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 electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	**x**		
Functional Safety Requirement 01-02	The electronic power steering ECU 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**		
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that the lane keeping assistance torque is below Max_Lane_Keep_Torque.	**x**		
Functional Safety Requirement 02-03	The electronic power steering ECU shall ensure that the lane keeping assistance applies no torque when the driver steering torque exceeds Max_Drifting_Torque.	**x**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Lane Assistance turned off until the vehicle is restarted.	Malfunction_01 Malfunction_02 Malfunction_04	Yes	Activate a warning symbol on Car Display indicating that the Lane Assistance item has been turned off.
WDC-02	LKA is deactivated for a duration of LKA_Deactivation_Period.	Malfunction_03	Yes	1. Activate a warning symbol on the Car Display indicating that LKA is deactivated. 2. Sound an alarm signal.
WDC-03	LKA is deactivated for a duration of LKA_Deactivation_Period, measured from the most recent triggering.	Malfunction_05	Yes	Activate a warning symbol on the Car Display indicating that LKA is deactivated.