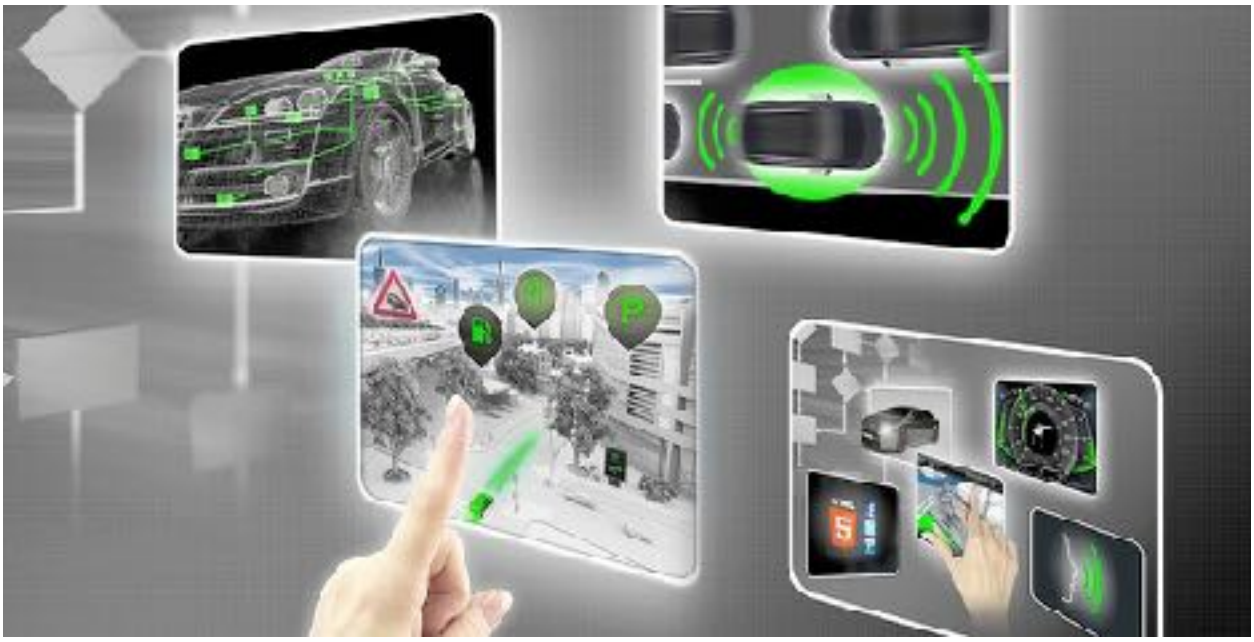
Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
2/24/2018	1.0	Huaping Gu	First version
3/4/2018	2.0	Huaping Gu	Rephrase and add move materials leant from lesson

Table of Contents

Purpose of the Functional Safety Concept

The functional safety concept is looking at the item from a higher level, not go into technical details. The functional safety concept looks at the general functionality of the item and specifies bellow information:

- the ASIL level
- the fault tolerant time interval, which measures how quickly a system needs to react to a hazardous situation
- And the safe state, which discusses what a system looks like after it has avoided an accident

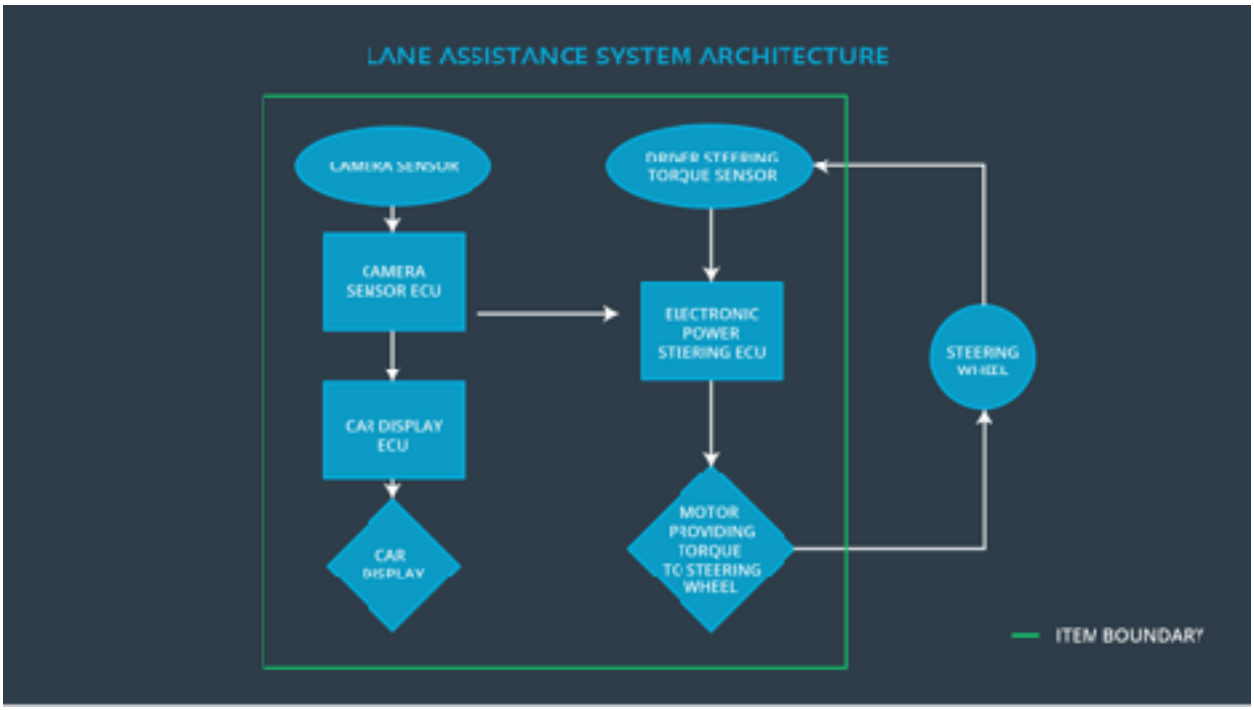
We are also going to discuss verification and validation, which is how you prove that a system actually meets your requirements.

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 assistance 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	Lane keeping assistance should be OFF when Camera ECU not function as expected.
Safety_Goal_04	Lane keeping assistance should be OFF when park off road.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	The camera sensor reads in images from the road.
Camera Sensor ECU	The camera sensor ECU identifies when the vehicle has accidentally departed its lane, and sent the appropriate messages to he car display ECU and the electronic Power steering ECU.
Car Display	Display lane departing warning signal on the display with text or image on the display screen.
Car Display ECU	Connect to Camera sensor ECU to get land
Driver Steering Torque Sensor	Sense the torque on the wheel.
Electronic Power Steering ECU	The Electronic Power Steering ECU receive the signal from Camera Sensor ECU and the Driver Steering Torque Sensor, then apply torque to the steering wheel accordingly.
Motor	The electrical component which generates the torque force based on the ECU signal 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 limited haptic feedback	MORE	The lane departure warning function applies an oscillating torque with very high torque amplitude (above limit)
Malfunction_02	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.
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	WRONG	Camera ECU subsystem has give wrong signal that the vehicle is off the lane while it is NOT
Malfunction_04	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	WRONG	Lane keeping LKA still function with unnecessary steering torque when car is parked off road.

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 oscillating steering torque from the lane departure warning function shall ensure that the lane departure oscillating torque amplitude is bellow Max_Torque_Amplitude.	C	50ms	Torque amplitude is bellow Max_Torque_Amplitude.

Functional Safety Requirement 01-02	The oscillating steering torque from the lane departure warning function shall ensure that the lane departure oscillating torque frequency is bellow Max_Torque_Frequency.	C	50ms	Torque frequency is bellow Max_Torque_Frequency.

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 the Max_Torque_**Amplitude** used is within the reasonable range where driver can detected and not impact driver's normal driving.	Verify that the system is been turn off if the LPW exceeded the Max_Torque_**Amplitude**
Functional Safety Requirement 01-02	Validate the Max_Torque_**Frequency** used is within the reasonable range where driver can detected and not impact driver's normal driving.	Verify that the system is been turn off if the LPW exceeded the Max_Torque_**Frequency**

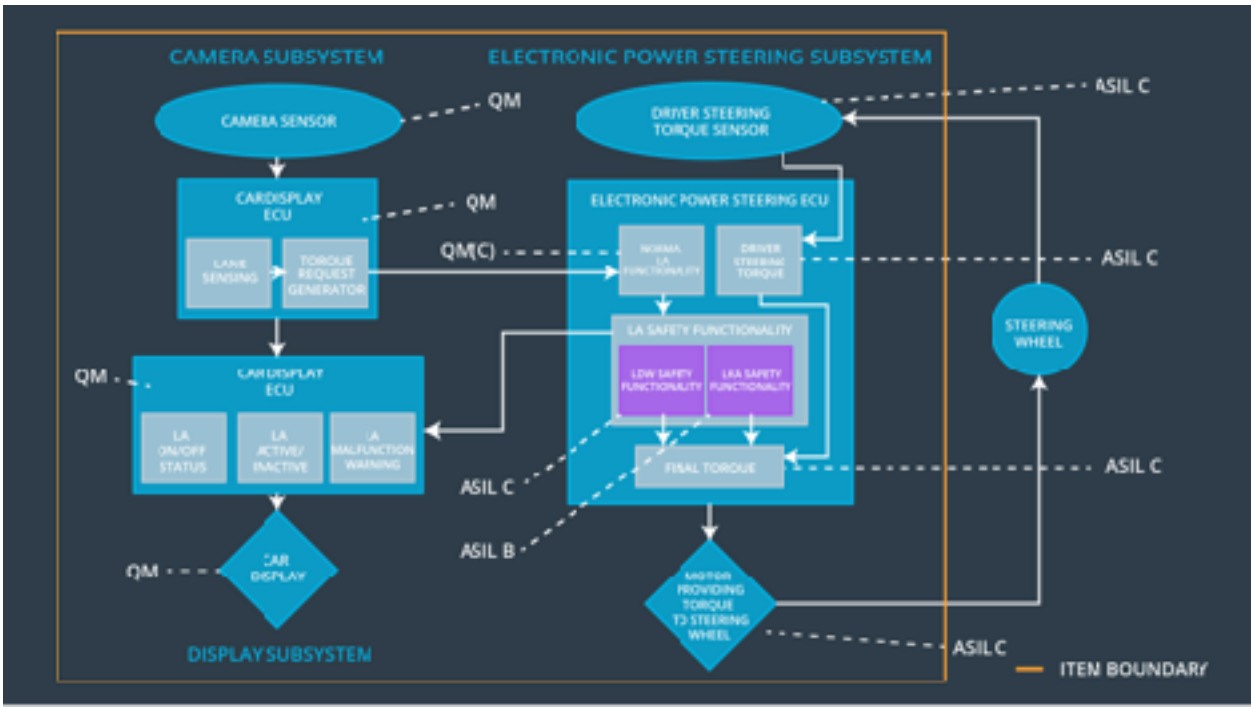
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The LKA shall ensure that the Lane Keeping Assistance torque is applied within Max_Duration.	B	50ms	The lane keeping assistance function is limited in time duration which prevents misuse as an autonomous driving function.
Functional Safety Requirement 03-01	The LKA shall automatically OFF when the camera ECU work incorrectly	A	50ms	LKA automatically OFF when it detects the camera ECU is not work.
Functional Safety Requirement 04-01	The LKA shall automatically OFF when the car is parked off road.	QM	500ms (Since vehicle is parked, no need to be shorter interval)	LKA automatically OFF when the car is parked off road.

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 LKA can automatically OFF when it is ON for a period of Max_Duration if driver's hands off the wheel, and can give warning messages to driver.	Verify that the LKA is OFF after a Max_Duration. If user's hands always on the steering wheel, LKA keep working.
Functional Safety Requirement 03-01	The LKA can automatically OFF when the camera ECU not work correctly.	Verify that the LKA is OFF when the Camera ECU not work.
Functional Safety Requirement 04-01	The LKA can automatically OFF when vehicle parked off road.	Verify LKA is OFF when the car is parked off road.

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 oscillating steering torque from the lane departure warning function shall ensure that the lane departure oscillating torque amplitude is bellow Max_Torque_Amplitude.	X		
Functional Safety Requirement 01-02	Validate the Max_Torque_Frequency used is within the reasonable range where driver can detected and not impact driver's normal driving.	X		
Functional Safety Requirement 02-01	The LKA can automatically OFF when it is ON for a period of Max_Duration if driver's hands off the wheel, and can give warning messages to driver.	X		
Functional Safety Requirement 03-01	The LKA can automatically OFF when the camera ECU not work correctly.	X		
Functional Safety Requirement 04-01	The LKA can automatically OFF when vehicle parked off road.	X		

Warning and Degradation Concept

[Instructions: Fill in the warning and degradation concept.]

For the lane assistance item, we discussed that the driver will see a warning light on the dashboard when the system malfunctions.
The lane departure warning and lane keeping assistance functionality will degrade by turning the system off. In other words, the torque request from the lane keeping assistance will be set to zero.

Degradation mode describes how the vehicle will be taken to a safe state when there is a malfunction. For the lane departure warning function, the degradation mode is to turn off the functionality. For the lane keeping assistance function, the degradation mode is the same.

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Lane Departure warning function will be OFF	Malfunction_01	Yes	Warning message of the lane Departure will be shown on the Vehicle Display screen
WDC-02	Lane keeping assistance function will be OFF	Malfunction_02 Malfunction_03 Malfunction_04	Yes	Warning message of the lane keeping assistance will be shown on the Vehicle Display screen