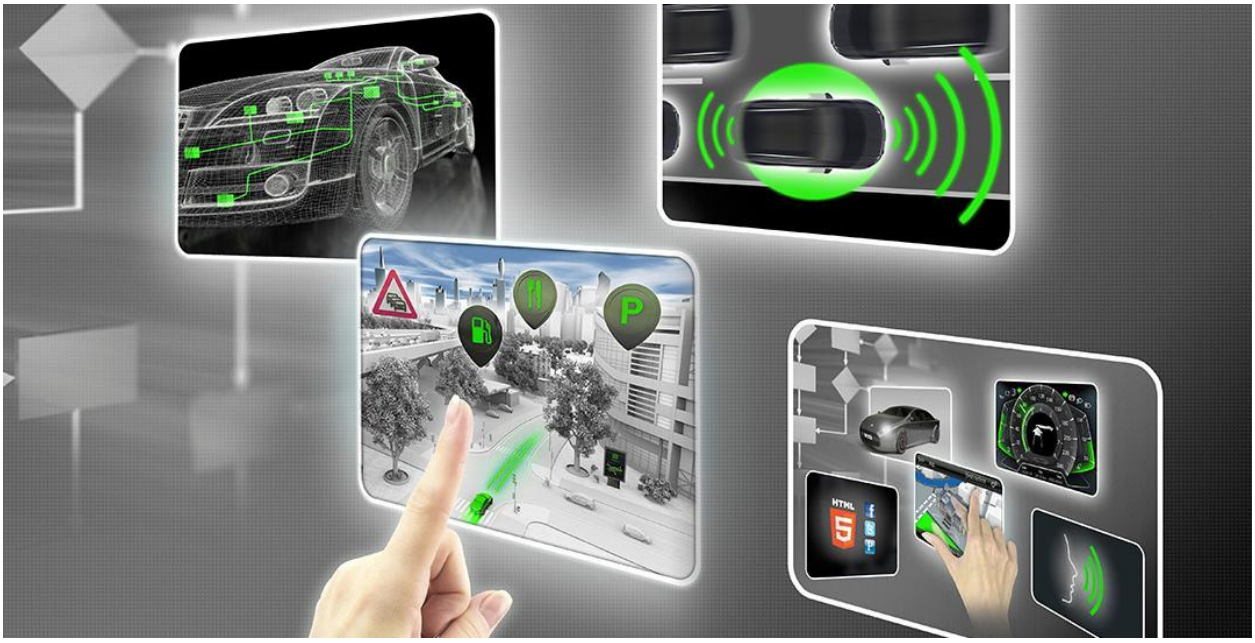
Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [Version]
Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
12/2/2017	1.0	Eric Lavigne	Initial Draft

12/18/2017	1.1	Eric Lavigne	Respond to review: clarify purpose and warning/degredation trigger

Table of Contents

Purpose of the Functional Safety Concept

The purpose of a functional safety concept is to derive high-level requirements from safety goals and then allocate requirements to sub-systems in the high-level architecture. These high-level requirements reduce the risks, associated with safety goals in the HARA, to acceptable levels.

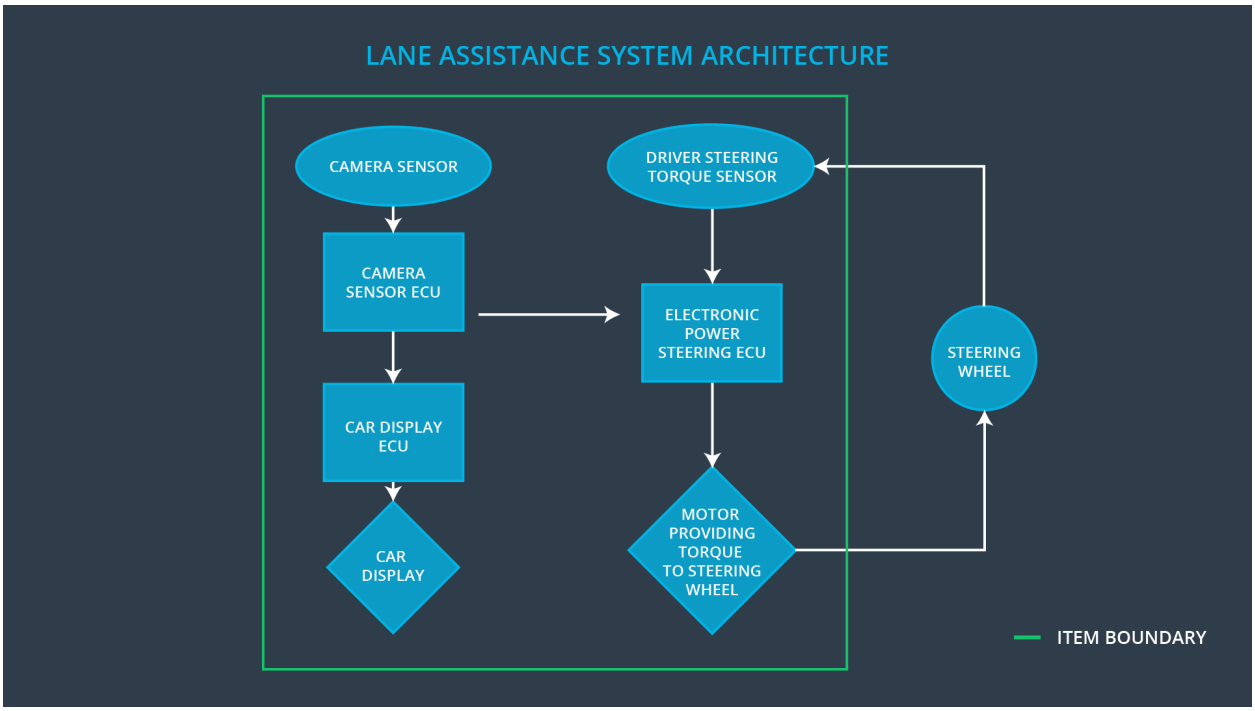
Inputs to the Functional Safety Concept

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

	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.

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 sends the appropriate messages to the Car Display ECU and the Electronic Power Steering ECU. (consider more detail on each of those messages)
Car Display	Shows the driver whether each lane assistance function is currently operating and warnings when a lane departure is in progress or when the lane keeping function will automatically disengage soon.

Car Display ECU	The car display ECU determines what information is displayed to the driver, including which lane assistance functions are currently operating and warnings about lane departure or impending disengagement of lane keeping.
Driver Steering Torque Sensor	The driver steering torque sensor determines how much torque the driver is applying to the steering wheel and sends that information to the electronic power steering ECU. This is needed primarily to make power steering work at all. In the lane assistance function, it can also be used to identify when the driver is attempting to override the lane assistance.
Electronic Power Steering ECU	The electronic power steering ECU determines the appropriate torque to apply to the steering wheel. This includes primarily amplification of torque applied by the driver, but also includes the primary behaviors of the lane assistance item: high-frequency variations for haptic feedback in the lane departure warning function and gentle turning for the lane keeping function.
Motor	The motor provides torque to the steering wheel to keep the car within its lane as part of the lane keeping function and applies high-frequency varying torque for haptic feedback as part of the lane departure warning function.

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 electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 ms	The LDW system will completely stop applying haptic feedback. Warning will display on dashboard informing driver of the fault.
Functional Safety	The electronic power steering ECU shall ensure that the lane departure oscillating	C	50 ms	The LDW system will completely

Requirement 01-02	torque frequency is below Max_Torque_Frequency.			stop applying haptic feedback. Warning will display on dashboard informing driver of the fault.

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	Confirm that safety drivers can easily maintain control with the chosen Max_Torque_Amplitude.	Deliberately insert a software fault that causes a high torque amplitude, then verify that the lane departure detection function turned off and that an appropriate warning appeared on the dashboard.
Functional Safety Requirement 01-02	Confirm that safety drivers can easily maintain control with the chosen Max_Torque_Frequency.	Deliberately insert a software fault that causes a high torque frequency, then verify that the lane departure detection function turned off and that an appropriate warning appeared on the dashboard.

Lane Keeping Assistance (LKA) Requirements:

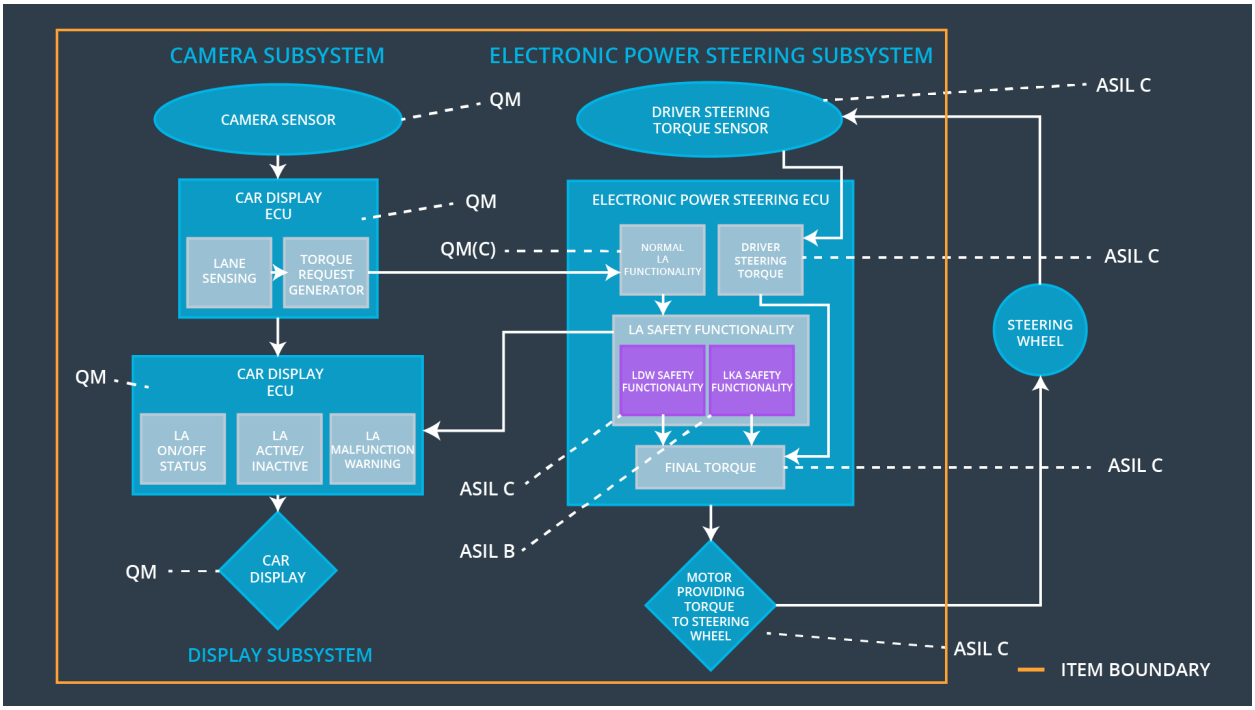
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500 ms	The LDW system will completely stop affecting the car steering. Warning will display on dashboard informing driver

				that lane keeping has stopped.

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	Confirm that the selected max_duration dissuades drivers from taking their hands off the wheel.	Validate that the lane keeping function turns off, with appropriate dashboard warning, when max_duration is exceeded.

Refinement of the System Architecture



Allocation of Functional Safety Requirements to Architecture Elements

ID	Functional Safety Requirement	Electronic Power Steering	Camera ECU	Car Display ECU

		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**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off functionality.	The lane departure warning function applies an oscillating torque with very high torque amplitude and/or frequency (above limit).	Yes	Warning indicator on dashboard
WDC-02	Turn off functionality.	The lane keeping assistance function is not limited in time duration which leads to misuse as an autonomous driving function.	Yes	Warning indicator on dashboard