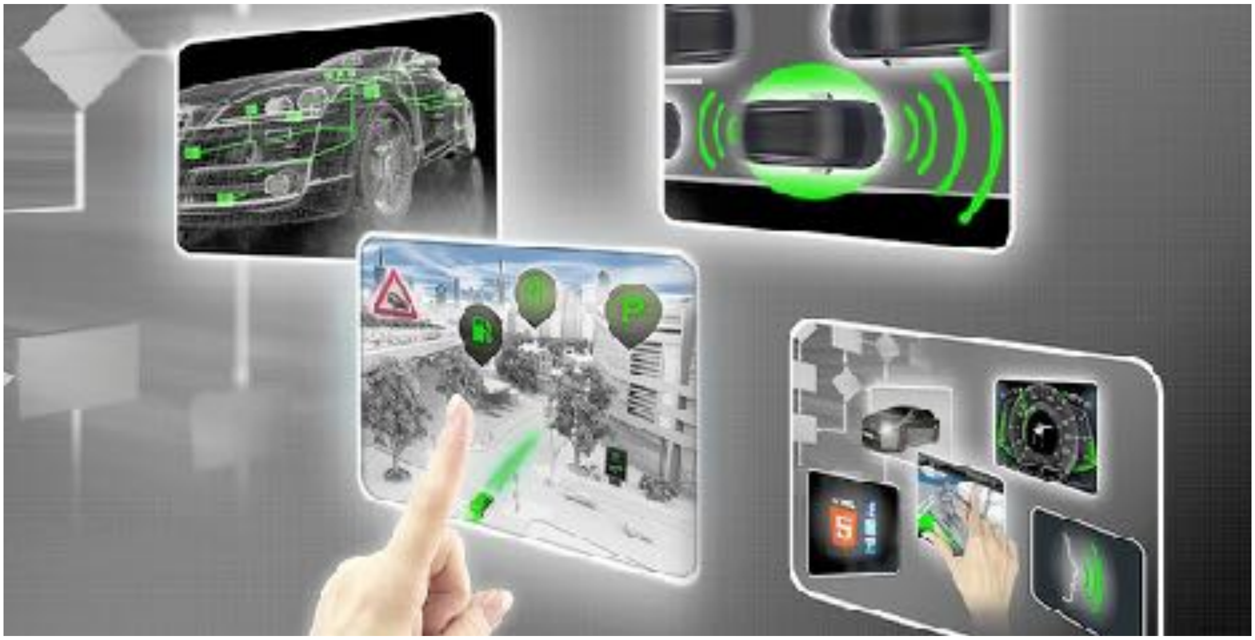
Functional Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
2/24-26/2018	1.0	Mark	Filling out Document while following class

Table of Contents

Purpose of the Functional Safety Concept

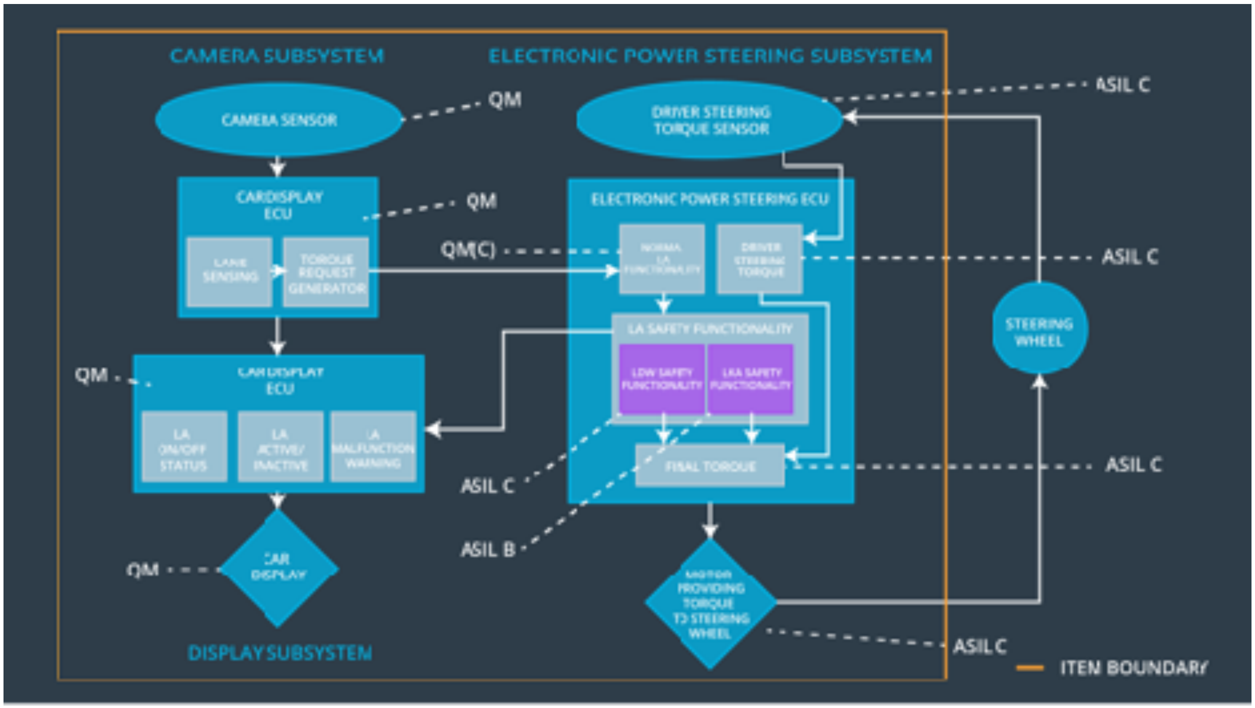
The functional safety concept is the final step in the “design” (left) side of the V in the ISO-26262 development lifecycle. Since it is also at the bottom of the V, it is focused on sub-systems and provides a high-level overview, for design purposes and helps guides the technical safety concept to ask the right questions and zero in on the right details to ensure safety.

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 LKA 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 LKA should turn off when the car’s tire system is abnormal.
Safety_Goal_04	No change needed, the probability and controllability combined help keep the ASIL to be QM.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Detecting lane lines and when the vehicle leaves the ego lane by mistake
Camera Sensor ECU	Alerting the Car Display and Electronic Power Steering ECUs as to lane-status (if there is a lane-departure)
Car Display	Displays to driver lane-departure warning sign
Car Display ECU	Controls turning on the warning sign based on alert from the Camera ECU
Driver Steering Torque Sensor	Detects driver’s input to the wheel (and lack of)
Electronic Power Steering ECU	Measures the torque and determines amount to change based on lane assistance toque request
Motor	Taking input from Electronic Power Steering ECU to apply the requested torque change (and safely, within limits)

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 LDW is giving MORE torque than what is safe	The LDW function applies an oscillating toque 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 LDW is giving MORE torque than what is safe	The LDS function applies an oscillating toque 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 LKA 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	50ms	The LDW turns off to stop applying the amplitude
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	The LDW turns off to stop applying the amplitude

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	We need to validate that the max_amplitude torque oscillation is safe enough for majority of drivers	When the max_amplitude crosses the limit, LDW is shut off.
Functional Safety Requirement 01-02	We need to validate that the max_frequency torque oscillation is safe enough for majority of drivers	When the max_frequency crosses the limit, LDW is shut off.

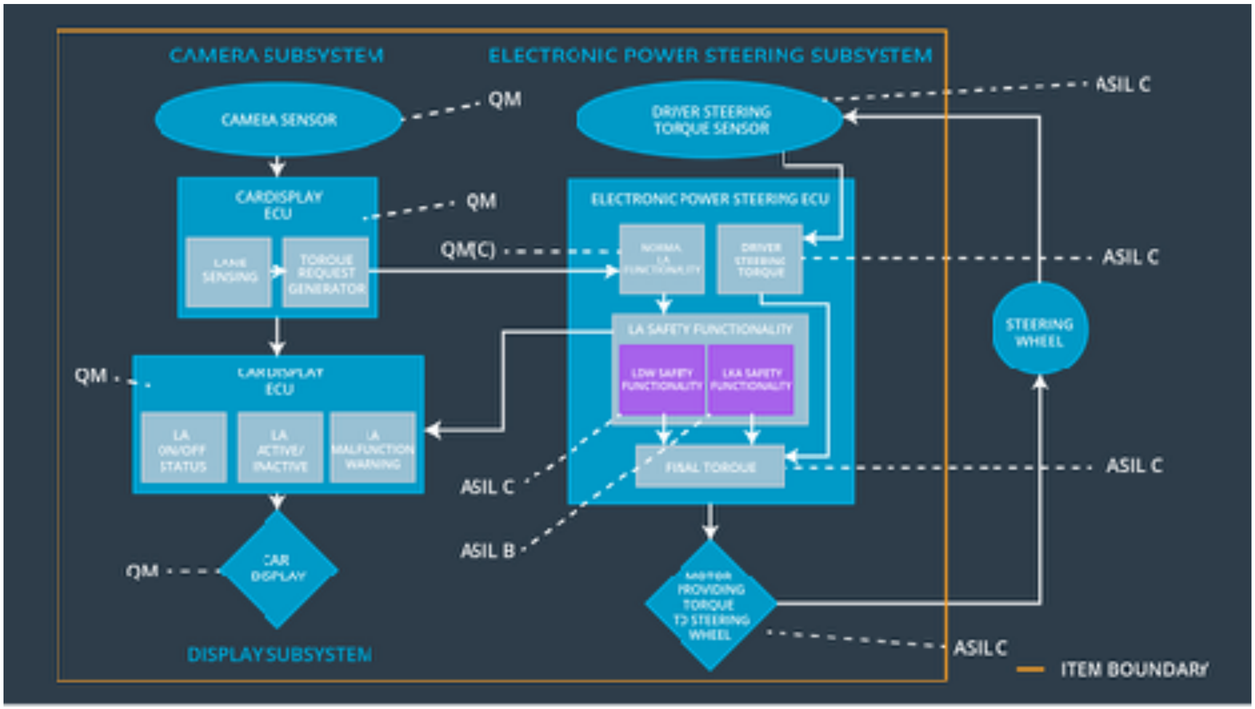
Lane Keeping Assistance (LKA) Requirements:

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 LKA torque is applied for only Max_Duration.	C	500ms	The LKA should turn off and the driving remain in control of car.

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 really does dissuade drivers from taking their hands off the wheel. (fun side note: could start playing The Doors song, “keep your eyes on the road and your hands upon the wheel”). Apologies, this is the only hidden “easter egg" joke in all these documents.	Verification will assure than when max_duration is exceeded, the LKA will turn off.

Refinement of the System Architecture



Allocation of Functional Safety Requirements to Architecture Elements

[Instructions: Mark which element or elements are responsible for meeting the functional safety requirement. Hint: Only one ECU is responsible for meeting all of the requirements.]

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-01	Electronic Power Steering ECU shall ensure that the LDW oscillating torque amplitude is below Max_Torque_Amplitude	**X**		
Functional Safety Requirement 01-02	Electronic Power Steering ECU shall ensure that the LDW oscillating torque frequency is below Max_Torque_Frequency	**X**		
Functional Safety Requirement 02-01	Electronic Power Steering ECU shall ensure that the LKA 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	Shut down LDW functionality	Steering wheel oscillation frequency or amplitude exceeds parameters	Yes	Warning icon displayed on Dashboard
WDC-02	Shut down LKA functionality	LKA functionality applies torque for longer than max_duration.	Yes	Warning icon displayed on Dashboard