Technical Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
12-05-2018	1.0	Fuqiang Huang	First Attempt for Submission

Table of Contents

Table of Contents

Document history 2

Table of Contents 2

Purpose of the Technical Safety Concept 3

Inputs to the Technical Safety Concept 4

Functional Safety Requirements 4

Refined System Architecture from Functional Safety Concept 5

Functional overview of architecture elements 5

Technical Safety Concept 7

Technical Safety Requirements 7

Refinement of the System Architecture 11

Allocation of Technical Safety Requirements to Architecture Elements 11

Warning and Degradation Concept 11

Purpose of the Technical Safety Concept

The Technical Safety Concept involves:

- Turning functional safety requirements into technical safety requirements.
- Allocating technical safety requirements to the system architecture.

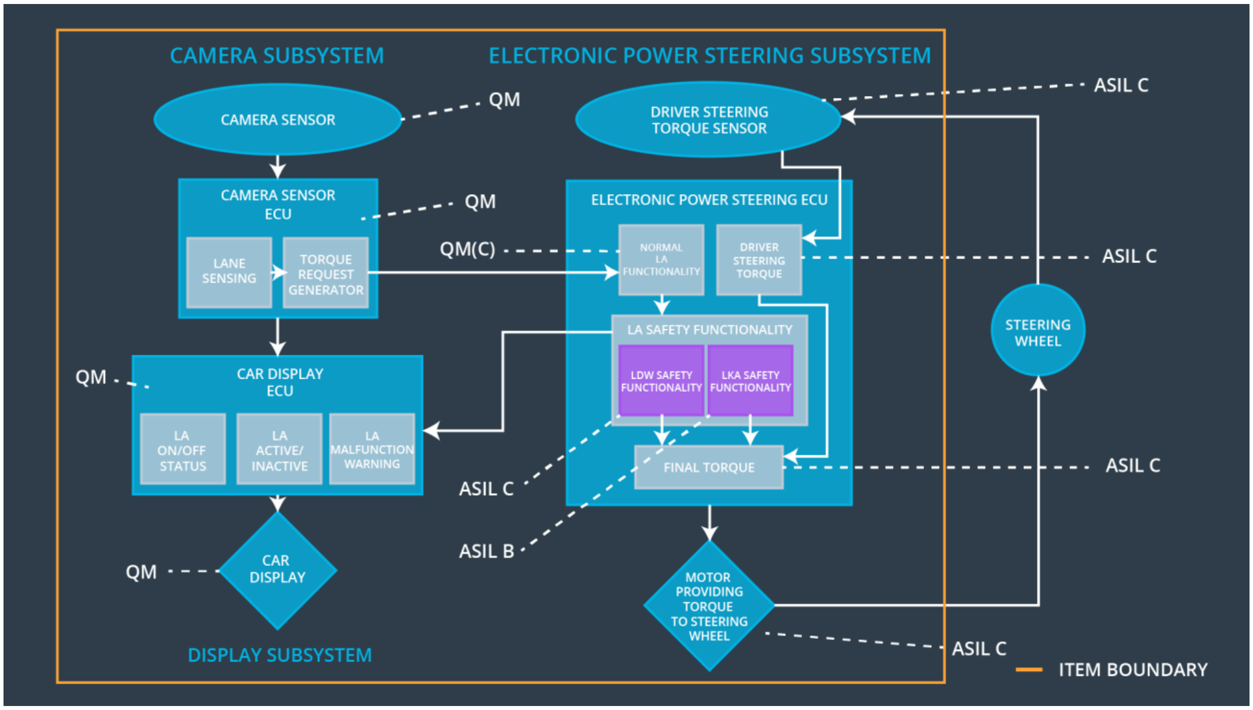
Unlike that the functional safety concept considers an item from a bird's eye view, the technique safety concept is more concrete, looking at the safety requirements of sensors, control unit, and actuators, and gets into the details of the item's technology. It provides a safety guideline for drilling down into hardware and software implementation.

Inputs to the Technical Safety Concept

Functional Safety 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	Oscillation torque amplitude is below Max_Torque_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	50 ms	Oscillation frequency is below Max_Torque_Frequency.
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	Lane Keeping Assistance torque is zero.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Captures road and vehicle images for the Camera Sensor ECU.
Camera Sensor ECU - Lane Sensing	Detects lane departures based on images captured
Camera Sensor ECU - Torque request generator	Sends a signal to the electronic power steering system asking to turn and vibrate the steering wheel, and requests a warning light in the car display dashboard.
Car Display	Provides a warning light in the car display dashboard to let the driver know whether the lane assistance system is active, and provides a button on the dashboard so that the driver can turn off the system completely if in need.
Car Display ECU - Lane Assistance On/Off Status	Gets the request signal from the Camera Sensor ECU to control the warning light.
Car Display ECU - Lane Assistant	Receives the on/off commands from the Car

Active/Inactive	Display to ask for activating/deactivating the assistance system.
Car Display ECU - Lane Assistance malfunction warning	Gets the request signal from EPS ECU to show malfunction warning on the driver dashboard.
Driver Steering Torque Sensor	Detects how much the driver is already turning the steering wheel.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Receives the driver steering torque from Driver Steering Torque Sensor.
EPS ECU - Normal Lane Assistance Functionality	Contains code for normal functional behavior.
EPS ECU - Lane Departure Warning Safety Functionality	Takes care of functional safety requirements of LDW.
EPS ECU - Lane Keeping Assistant Safety Functionality	Takes care of functional safety requirements of LKA.
EPS ECU - Final Torque	Calculates the final torque based on the driver steering torque and safety functionality of LDW and LKA.
Motor	Vibrates the steering wheel to give a warning to the driver based on the information from Electronic Power Steering ECU, and applies the extra torque to the steering wheel to draw the vehicle back to the center of the lane.

Technical Safety Concept

Technical Safety Requirements

Lane Departure Warning (LDW) Requirements:

Functional Safety Requirement 01-01 with its associated system elements
(derived in the functional safety concept)

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		

Technical Safety Requirements related to Functional Safety Requirement 01-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	The LDW safety component shall ensure that the amplitude of the 'LDW_Torque_Request' sent to the 'Final electronically power steering Torque' component is below 'Max_Torque_Amplitude'.	C	50 ms	LDW Safety	LDW torque output is set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	N/A
Technical Safety Requirement 03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW_Torque_Request' shall be set to zero.	C	50 ms	LDW Safety	LDW torque output is set to zero

Technical Safety Requirement 04	As soon as the LDW function deactivates the LDW feature, the LDW Safety software block shall send a signal to the car display ECU to turn on a warning light.	C	50 ms	LDW Safety	LDW torque output is set to zero
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	LDW torque output is set to zero

Functional Safety Requirement 01-2 with its associated system elements (derived in the functional safety concept)

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	X		

Technical Safety Requirements related to Functional Safety Requirement 01-02 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	The LDW safety component shall ensure that the frequency of the 'LDW_Torque_Request' sent to the 'Final electronically power steering Torque' component is below 'Max_Torque_Frequency'.	C	50 ms	LDW Safety	LDW torque output is set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	N/A

Technical Safety Requirement 03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW_Torque_Request' shall be set to zero.	C	50 ms	LDW Safety	LDW torque output is set to zero
Technical Safety Requirement 04	As soon as the LDW function deactivates the LDW feature, the LDW Safety software block shall send a signal to the car display ECU to turn on a warning light.	C	50 ms	LDW Safety	LDW torque output is set to zero
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	LDW torque output is set to zero

Lane Keeping Assistance (LKA) Requirements:

Functional Safety Requirement 02-1 with its associated system elements (derived in the functional safety concept)

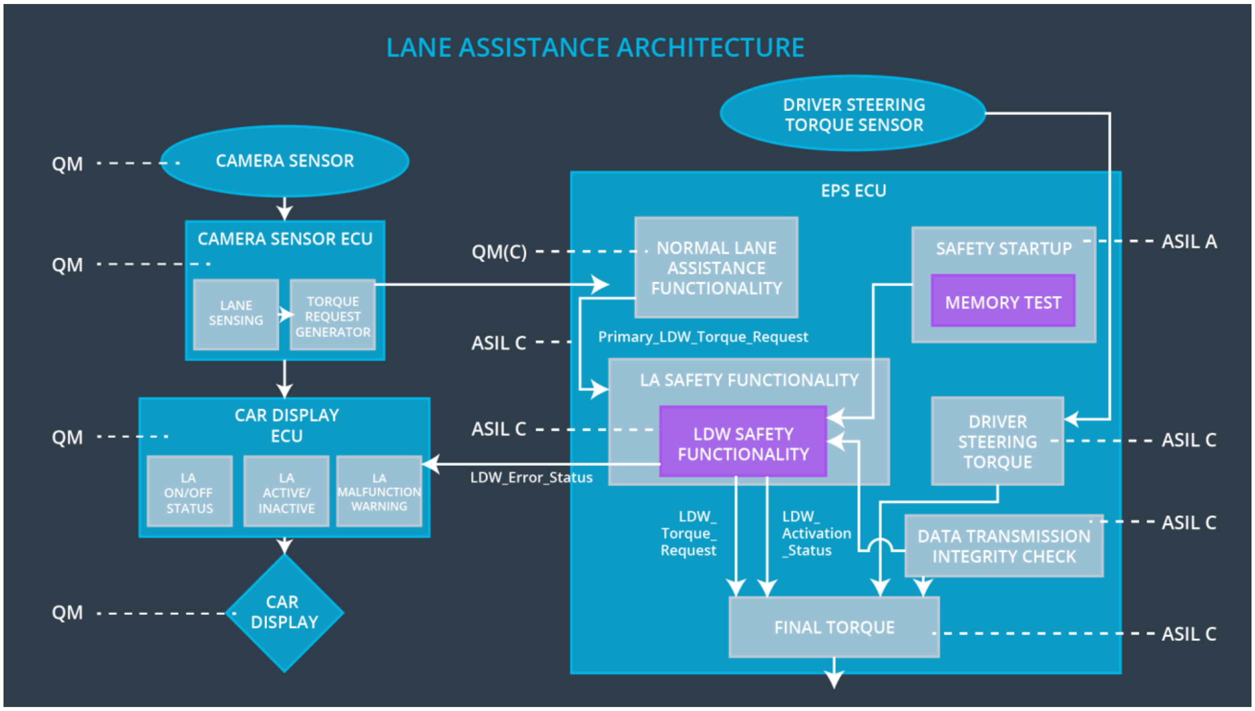
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement	The LKA safety component shall ensure that the duration of the 'LKA_Torque_Request' sent	B	500 ms	LKA Safety	LKA torque output is set to zero

01	to the 'Final electronically power steering Torque' component is below 'Max_Torque_Duration'.				
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500 ms	Data Transmission Integrity Check	N/A
Technical Safety Requirement 03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the 'LKA_Torque_Request' shall be set to zero.	B	500 ms	LKA Safety	LKA torque output is set to zero
Technical Safety Requirement 04	As soon as the LKA function deactivates the LKA feature, the LKA Safety software block shall send a signal to the car display ECU to turn on a warning light.	B	500 ms	LKA Safety	LKA torque output is set to zero
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	LKA torque output is set to zero

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

For this particular item, all technical safety requirements are allocated to the Electronic Power Steering ECU.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the functionality.	Malfunction_01 Malfunction_02	Yes	Warning light on the dashboard
WDC-02	Turn off the functionality.	Malfunction_03	Yes	Warning light on the dashboard