Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 2.0

Template Version 1.0, Released on 2017-06-21

Document history

[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description
11/12/2017	1.0	Sam Adelman	Begin assignment
11/26/2017	2.0	Sam Adelman	Added information from lessons

Table of Contents

[Instructions: We have provided a table of contents. If the table of contents is not showing up correctly in your word processor of choice, please update it. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In Google Docs, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]

Purpose of the Technical Safety Concept

The technical safety concept involves:

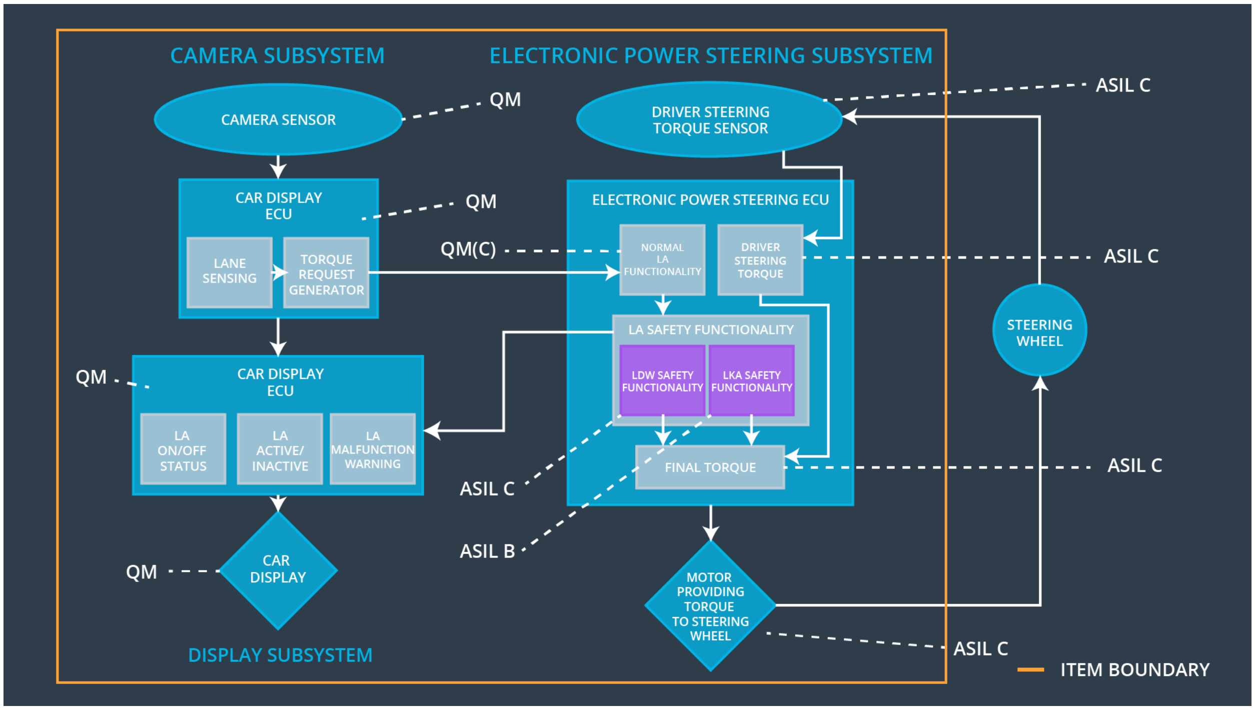
- Turning functional safety requirements into technical safety requirements
- Allocating technical safety requirements to the system architecture

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	Torque request set to zero
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	Torque request set to zero
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 disengages, no corrective steering torque applied

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Captures images of the lane
Camera Sensor ECU - Lane Sensing	Finds relative position of vehicle in lane from Camera Sensor input
Camera Sensor ECU - Torque request generator	Generates oscillating torque request if vehicle is drifting out of its lane
Car Display	Provides visual feedback to driver
Car Display ECU - Lane Assistance On/Off Status	Indicates to driver if the LKA system is on or off.
Car Display ECU - Lane Assistant Active/Inactive	Indicates to driver if the LKA has detected that the vehicle is drifting out of its lane
Car Display ECU - Lane Assistance malfunction warning	Indicates to the driver a malfunction in the LKA system
Driver Steering Torque Sensor	Detects current steering torque input from driver

	using the steering wheel.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Receives information from Driver Steering Torque Sensor about the steering torque provided by the driver via the steering wheel
EPS ECU - Normal Lane Assistance Functionality	Provides EPS functionality during normal driving when the LDW system does not detect lane departure
EPS ECU - Lane Departure Warning Safety Functionality	Processes haptic feedback to the user from the torque request generator when the LDW system detects lane departure
EPS ECU - Lane Keeping Assistant Safety Functionality	Limits the haptic feedback to the user when from the torque request generator to remain below the Max_Torque_Amplitude and Max_Torque_Frequency.
EPS ECU - Final Torque	Final torque request sent out to the Motor providing torque to the steering wheel
Motor	Actuator that provides torque to the steering wheel.

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 electronic power steering Torque' component is below 'Max_Torque_Amplitude.	C	50 mS	LDW Safety Software Component	Torque amplitude below maximum
Technical Safety Requirement 02	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 Software Component	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 Software Component	Torque set to zero
Technical Safety Requirement 04	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 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Safety Startup	N/A

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 amplitude of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_ Frequency.	C	50 mS	LDW Safety Software Component	Torque frequency below maximum
Technical Safety Requirement 02	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 Software Component	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 Software Component	Torque set to zero
Technical Safety Requirement 04	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 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Safety Startup	N/A

Lane Keeping Assistance (LKA) Requirements:

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

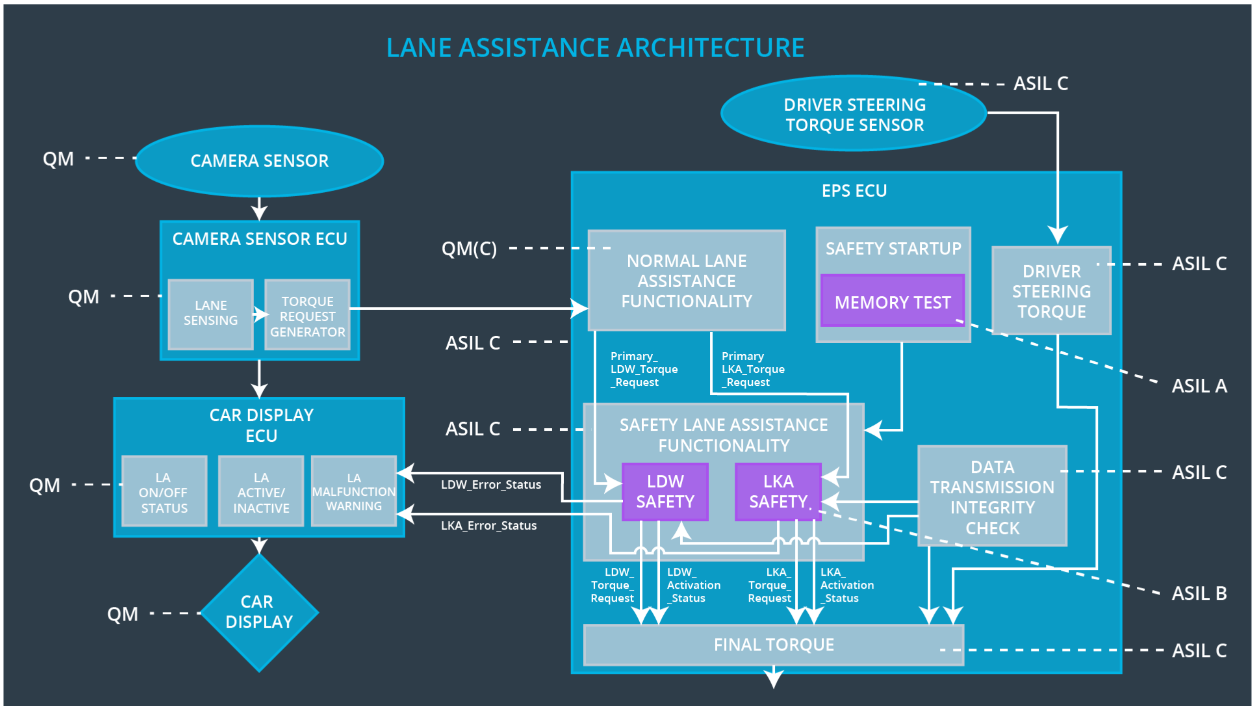
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The lane keeping assistance function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver can not misuse the system for autonomous driving.	B	500 ms	LKA Safety Software Component	Lane Keeping Assistance disengages, no corrective steering torque applied
Technical Safety Requirement 02	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 Software Component	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 Software Component	Torque set to zero
Technical Safety Requirement 04	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	Memory test shall be conducted at start up of the EPS ECU to	A	Ignition cycle	Safety Startup	N/A

Requirement 05	check for any faults in memory.				

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

Included above in the technical requirement tables. All technical safety requirements for this item 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 functionality	Vibration amplitude too high (+/- 3 N-m) or frequency too	Yes	Warning light

		high		
WDC-02	Turn off functionality	Lane keeping assistance duration exceeds Max_Duration	Yes	Warning light