Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: [Version]

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
29 Oct 2017	1.0	R Hariharan	Technical Safety Concept for Lane Assistance

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

[Instructions: Answer what is the purpose of a technical safety concept?]

Technical Safety Concept further refines the functional safety concept and it is part of Product Development phase. It is more concrete than Functional safety Document in terms of going into details of the Item's Technology requirements. Technical safety requirements are generated based on the functional safety requirements. These are then allocated to the system architecture. Validation and verification tests are provided for the technical requirements.

Inputs to the Technical Safety Concept

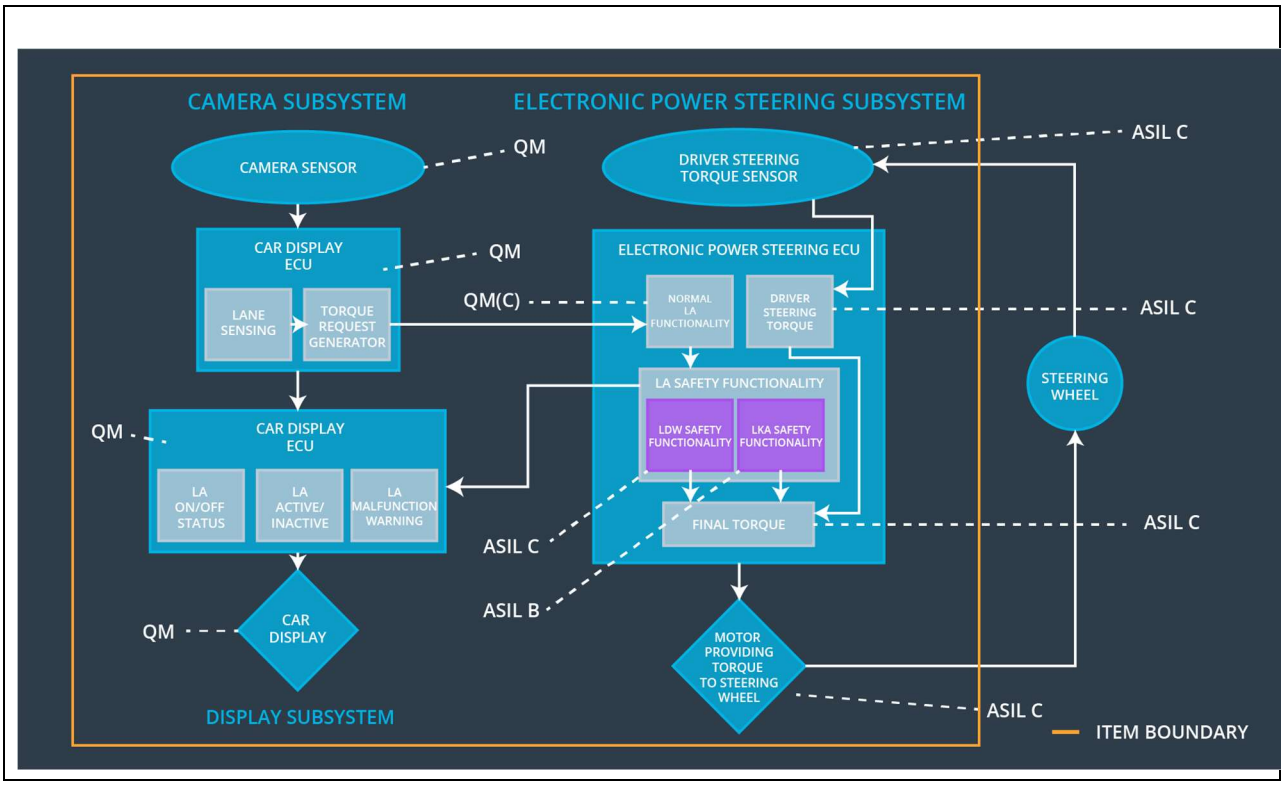
Functional Safety Requirements

[Instructions: Provide the functional safety requirements derived in the functional safety concept]

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	OFF
Functional Safety Requirement 01-02	"the electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency is below Max_Torque_Frequency". The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	OFF
Functional Safety Requirement 02-01	"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 cannot misuse the system for autonomous driving" The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500ms	OFF

Refined System Architecture from Functional Safety Concept

[Instructions: Provide the refined system architecture from the functional safety concept]



Functional overview of architecture elements

[Instructions: Provide a description for each functional safety element; what is each element's purpose in the lane assistance item?]

Element	Description
Camera Sensor	Physical sensor responsible for detecting lane lines And sends an image stream to the Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	Software and Hardware module which interprets sensor data and identifies lane markings in the image. Determines the position of the vehicle relative to the lane.
Camera Sensor ECU - Torque request generator	Sends torque request to Lane Assistance functionality
Car Display	Vehicle dashboard lights or display / screen unit

	providing status feedback to the driver of vehicle systems.
Car Display ECU - Lane Assistance On/Off Status	Provides feedback to the driver about on/off status of the Lane Assistance system
Car Display ECU - Lane Assistant Active/Inactive	Provides feedback to the driver about active/ inactive status of the Lane Assistance system
Car Display ECU - Lane Assistance malfunction warning	Provides feedback to the driver about malfunction status of the Lane Assistance system. Receives input from LDW Safety Functionality (LDW_Error_Status)
Driver Steering Torque Sensor	Physical sensor such as an encoder or strain gauge capable of measuring steering torque input on the steering wheel from the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	A hardware / software module on the Power Steering ECU which measures the signal from the Torque sensor and provides a software value of the driver steering torque.
EPS ECU - Normal Lane Assistance Functionality	Responsible for processing the input from the Camera Sensor ECU and sending Primary_LDW_Torque_Request to the LA Safety Functionality
EPS ECU - Lane Departure Warning Safety Functionality	A safety verified software module which monitors and passes through the output of the Normal Lane Assistance Functionality for faults related to safety requirements of the LDW function. (Such as max torque amplitude and frequency)
EPS ECU - Lane Keeping Assistant Safety Functionality	A safety verified software module which monitors and passes through the output of the Normal Lane Assistance Functionality for faults related to safety requirements of the LKA function. (Such as max_duration for torque output)
EPS ECU - Final Torque	A software value of the final torque which should be output to the Electronic Power Steering Motor based on the Lane Assistance Function and the driver input measured torque
Motor	Carries out the Electronic Power Steering ECU torque request and provides torque to the steering wheel

Technical Safety Concept

Technical Safety Requirements

[Instructions: Fill in the technical safety requirements for the lane departure warning first functional safety requirement. We have provided the associated functional safety requirement in the first table below. Hint: The technical safety requirements were discussed in the lesson videos. The architecture allocation column should contain element names such as LDW Safety block, Data Transmission Integrity Check, etc. Allocating the technical safety requirements to the "EPS ECU" does not provide enough detail for a technical safety concept.]

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	50ms	LDW Safety Functionality	OFF
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	50ms	LDW Safety Functionality	OFF
Technical Safety Requirem	As soon as a failure is detected by the LDW function, it shall	C	50ms	LDW Safety Functionality	OFF

ent 03	deactivate the LDW feature and the 'LDW_Torque_Request' shall be set to zero.				
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	Data Transmission integrity check	OFF
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	50ms	Safety Startup	OFF

[Instructions: Fill in the technical safety requirements for the lane departure warning second functional safety requirement. We have provided the associated functional safety requirement in the table below. Hint:. Most of the technical safety requirements will be the same. At least one technical safety requirement will have to be slightly modified because we are talking about frequency instead of amplitude. These requirements were not given in the lessons]

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	The LDW safety component shall ensure that the frequency of the	C	50ms	LDW Safety Functionality	OFF

Requirement 01	'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency				
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	50ms	LDW Safety Functionality	OFF
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	50ms	LDW Safety Functionality	OFF
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured	C	50ms	Data Transmission Integrity Check	OFF
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	50ms	Safety Startup	OFF

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]

Lane Keeping Assistance (LKA) Requirements:

[Instructions: Fill in the technical safety requirements for the lane keeping assistance functional safety requirement 02-01. We have provided the associated functional safety requirement in the table below. Hint:. You can reuse the technical safety requirements from functional safety requirement 01-01. But you need to change the language because we are now looking at a different system. The ASIL and Fault Tolerant Time Interval are different as well.]

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:

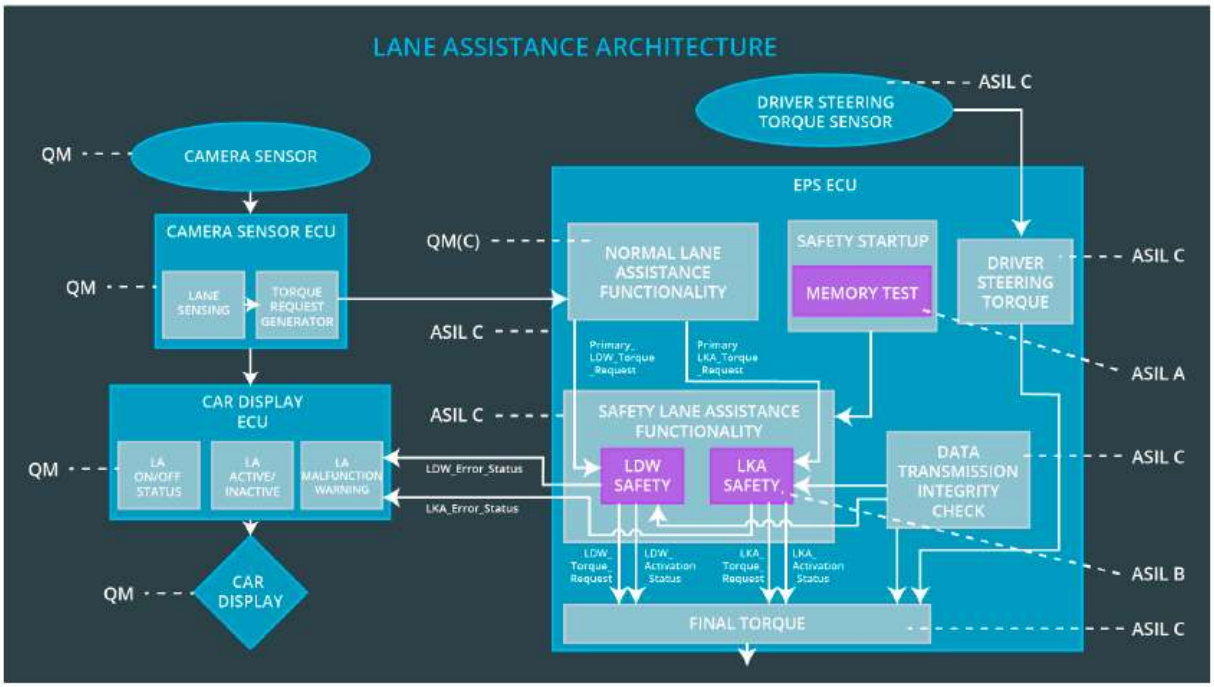
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LDW safety component shall ensure that the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is applied for only Max_Duration	B	500ms	LKA Safety Functionality	OFF
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	B	500ms	LKA Safety Functionality	OFF
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.	B	500ms	LKA Safety Functionality	OFF
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured	B	500ms	EPS ECU - Lane Keeping Assistance Safety Functionality, EPS ECU - Final Torque (Data integrity Check)	OFF
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition Time	EPS ECU Hardware	

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]

Refinement of the System Architecture

[Instructions: Include the refined system architecture. Hint: The refined system architecture should include the system architecture from the end of the technical safety lesson, including all of the ASIL labels.]



Allocation of Technical Safety Requirements to Architecture Elements

[Instructions: We already included the allocation as part of the technical requirement tables. Here you can state that for this particular item, all technical safety requirements are allocated to the Electronic Power Steering ECU]

For the Lane Keeping item, all technical safety requirements are allocated to the Electronic Power Steering ECU

Warning and Degradation Concept

[Instructions: We've already identified that for any system malfunction, the lane assistance functions will be turned off and the driver will receive a warning light indication. The technical safety requirements have not changed how functionality will be degraded or what the warning will be.

So in this case, the warning and degradation concept is the same for the technical safety requirements as for the functional safety requirements. You can copy the functional safety warning and degradation concept here.

Oftentimes, a technical safety analysis will lead to a more detailed warning and degradation concept.]

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	OFF	If Torque amplitude exceeds Max_Torque_Amplitude or Torque frequency exceeds Max_Torque_Frequency	YES	Warning light in car display
WDC-02	OFF	If LKA torque applied exceeds the Max_Duration time interval	YES	Warning light in car display