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
August 13, 2018	V 1.0	Li Gen	

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?]

- **Taking functional safety requirements into technical safety requirements;**
- **Allocating technical safety requirements to the system architecture.**

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 LDW item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Set the oscillation torque amplitude to zero
Functional Safety Requirement 01-02	The LDW item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	Set the oscillation torque amplitude to zero
Functional Safety Requirement 02-01	The LKA function item shall be time limiter and the additional steering torque shall end after a given time interval so that the driver can not misuse the system for autonomous driving.	B	500ms	Set the oscillation torque amplitude to zero

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	Hardware that get pattern information
Camera Sensor ECU - Lane Sensing	Input pattern information, after calculation, output lane sensing signal
Camera Sensor ECU - Torque request generator	Input calculation of lane sensing result, output torque request to EPS ECU
Car Display	Display warning information based on Camera Sensor ECU and EPS ECU
Car Display ECU - Lane Assistance On/Off Status	Show On/OFF status of Lane Assistance
Car Display ECU - Lane Assistant Active/Inactive	Show active/Inactive status of Lane Assistance
Car Display ECU - Lane Assistance malfunction warning	Show malfunction warning information of Lane Assistance
Driver Steering Torque Sensor	Detect driver steering torque, and output result to EPS ECU to decide hands on/off status.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Decided whether driver is hands on/off status based on driving steering torque sensor.
EPS ECU - Normal Lane Assistance Functionality	ECU for normal lane assistance working, send primary LDW torque request to safety lane assistance functionality.

EPS ECU - Lane Departure Warning Safety Functionality	Decide whether vehicle is out of lane center or not, if yes output signal to Display ECU to show warning information to driver, and also send vibration warning on steering wheel motor. Check primary LDW torque request is less than maximum torque or not.
EPS ECU - Lane Keeping Assistant Safety Functionality	If vehicle is out of lane, decided how much torque to get vehicle back to lane center, then send signal to final torque ECU of EPS
EPS ECU - Final Torque	Based on driver torque and EPS ECU input torque, to output a final torque request to Motor
Motor	Actuator, output steering torque based on EPS ECU final torque signal

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	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is	X		

01-01	below Max_Torque_Amplitude			

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	Lane departure warning torque request amplitude shall be set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured	C	50ms	Data Transmission integrity check	Lane departure warning torque request amplitude shall be set to zero
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	Lane departure warning torque request amplitude shall be 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	50ms	Lane Assist Malfunction warning	Lane departure warning torque request amplitude shall be set to zero
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	Same with engine ignition cycle	Safety setup block	Lane departure warning torque request

					amplitude shall be set to zero

[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 Requirement 01	The LDW safety component shall ensure that the frequency of the ‘LDW_Torque_Request’ sent to the ‘Final electronic power steering Torque’component is below ‘Max_Torque_Frequency’	C	50ms	LDW safety	Lane departure warning torque request amplitud

					e shall be set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for ‘LDW_Torque_Request’ signal shall be ensured	C	50ms	Data Transmission integrity check	Lane departure warning torque request amplitude shall be set to zero
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	Lane departure warning torque request amplitude shall be 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	50ms	Lane Assist Malfunction warning	Lane departure warning torque request amplitude shall be set to zero
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	Same with engine ignition cycle	Safety setup block	Lane departure warning torque request amplitud

					e shall be set to zero

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:

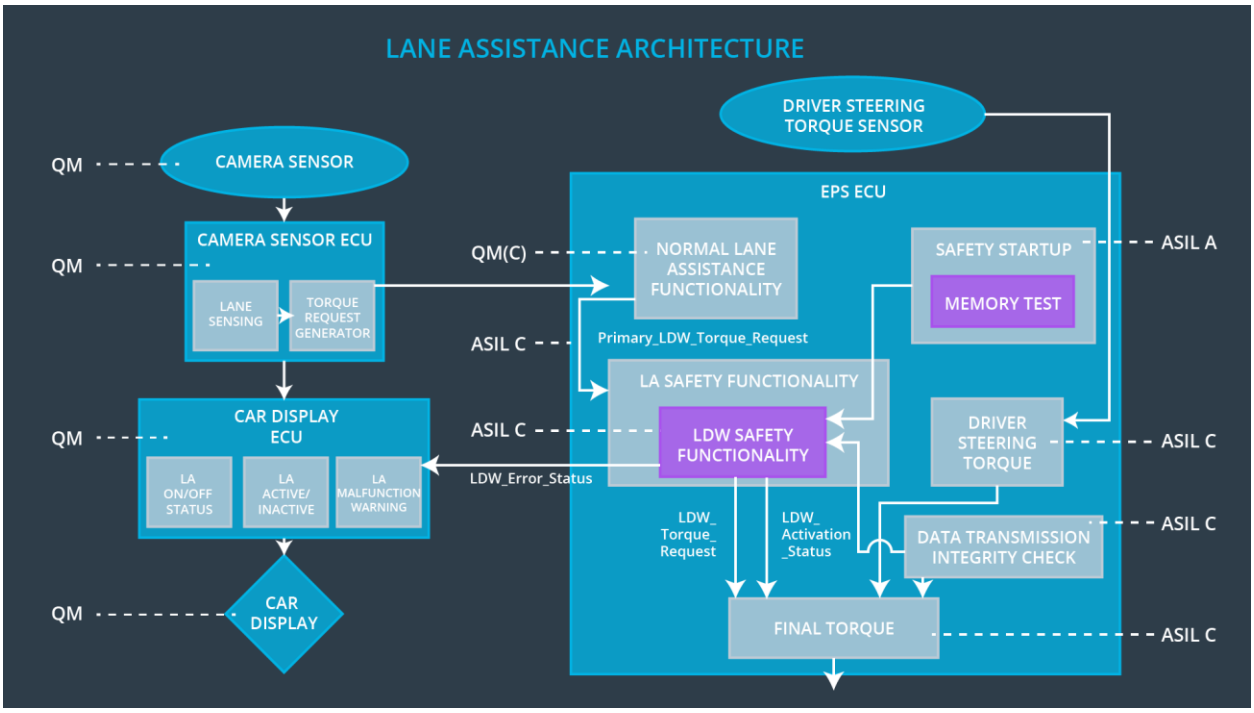
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LKA safety component shall ensure that the 'time_duration' of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque'component is below 'Max_Duration'	B	500ms	LKA safety block	Turn off the LKA system when malfunction.
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'time_duration' signal shall be ensured	B	500ms	Data Transmission integrity check	Turn off the LKA system when malfunction.
Technical Safety Requirement 03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the 'time_durationt' shall be set to zero	B	500ms	LKA safety	Turn off the LKA system when malfunction.
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	500ms	Lane Assist Malfunction warning	Turn off the LKA system when malfunction.
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	Same with engine ignition cycle	Safety setup block	Turn off the LKA system when malfunction.

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]

As most of element the LDW and LKA use the same one, and the principle is follow the highest ASIL level, so most ASIL level follow the LDW allocation architecture elements.

Some particular item need to be attention. The LKA safety functionality block should be ASIL B.

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.]

The lane assistance function is not autonomous driving function, driver should not be hands off.