Technical Safety Concept Lane Assistance

Document history

Date	Version	Editor	Description
6/22/2018	1.0	Jason Kang	First Draft

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

Inputs to the Technical Safety Concept
Functional Safety Requirements

The goal of this document is to determine take the functional safety requiements defined in the Functional Safety Concept and convert them into technical safety requirements. In addtition it lists other requirements invloving detecting faults, communications between different subsystems, methods for reaching a safe state, implementing warnings, and preventing latent faults. These are more focused requirements targeting the subsystems of the overall system. Furthermore, these technical safety requirements are assigned to a specific resource in the system architecture.

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Set Vibration Torque to 0
Functional Safety Requirement 01-02	The power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	Set Vibration Torque to 0
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	500ms	lane keeping assistance function disabled

Refined System Architecture from Functional Safety Concept
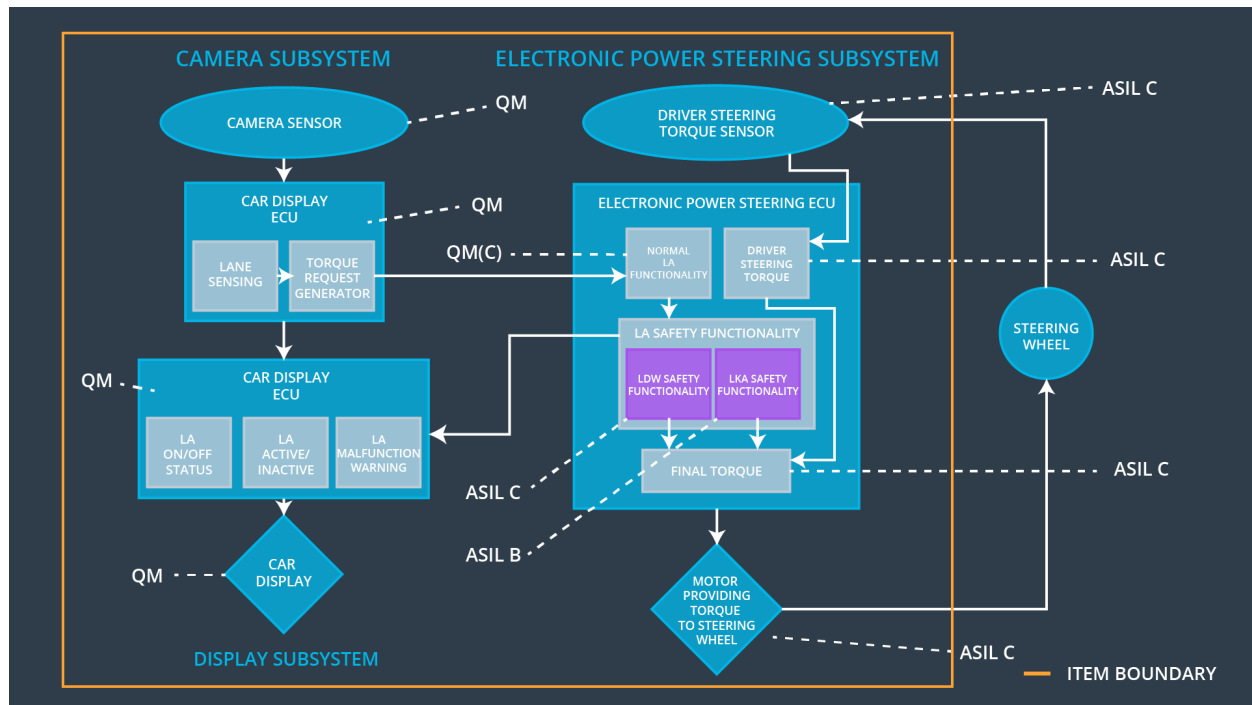
Functional overview of architecture elements

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

Element	Description
Camera Sensor	Visualizes the road in front of the vehicle.
Camera Sensor ECU - Lane Sensing	Determines the edges of the lane and heading, passes this information to other ECUs.
Camera Sensor ECU - Torque request generator	Recognizes that the driver is departing the lane. Requests activation of lane keeping assistant.
Car Display	Displays warning lights
Car Display ECU - Lane Assistance On/ Off Status	Lights up lane assistance indicator based on lane assistance state
Car Display ECU - Lane Assistant Active/Inactive	Lights up lane assistance indicator based on lane assistance state
Car Display ECU - Lane Assistance malfunction warning	Lights up if lane assistance malfunction indicator if a fault has occured.
Driver Steering Torque Sensor	Determines the amount of torque the driver is

	applying to the steering wheel
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Reads torque sensor to determine the amount of torque driver is applying
EPS ECU - Normal Lane Assistance Functionality	Monitors driver steering torque. Decides on whether or not to activate lane departure warning or lane keeping assistnt.
EPS ECU - Lane Departure Warning Safety Functionality	Decides how much vibration to apply to the steering wheel to warn of lane departure
EPS ECU - Lane Keeping Assistant Safety Functionality	Figures out how much assisting torque to apply to the steering wheel to help to maintaion lane
EPS ECU - Final Torque	Applies final limits on vibration amplitude and frequency.
Motor	Applies additional torque to the steering wheel per direction of the Power Steering ECU

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 electornic power steering Torque' component is less than '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 fo 'LDW_Torque_Request' signal shal be ensured	C	50ms	Data Transmission Integrity	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	LDW Safety	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	Ignition Cycle	Memory Test	Lane Departure Warning Torque Request Amplitude shall be 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 electornic power steering Torque' component is less than 'Max_Torque_Frequency'	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 fo 'LDW_Torque_Request' signal shal be ensured	C	50ms	Data Transmission Integrity	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	LDW Safety	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	Ignition Cycle	Memory Test	Lane Departure Warning Torque Request Amplitude shall be set to zero

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

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:

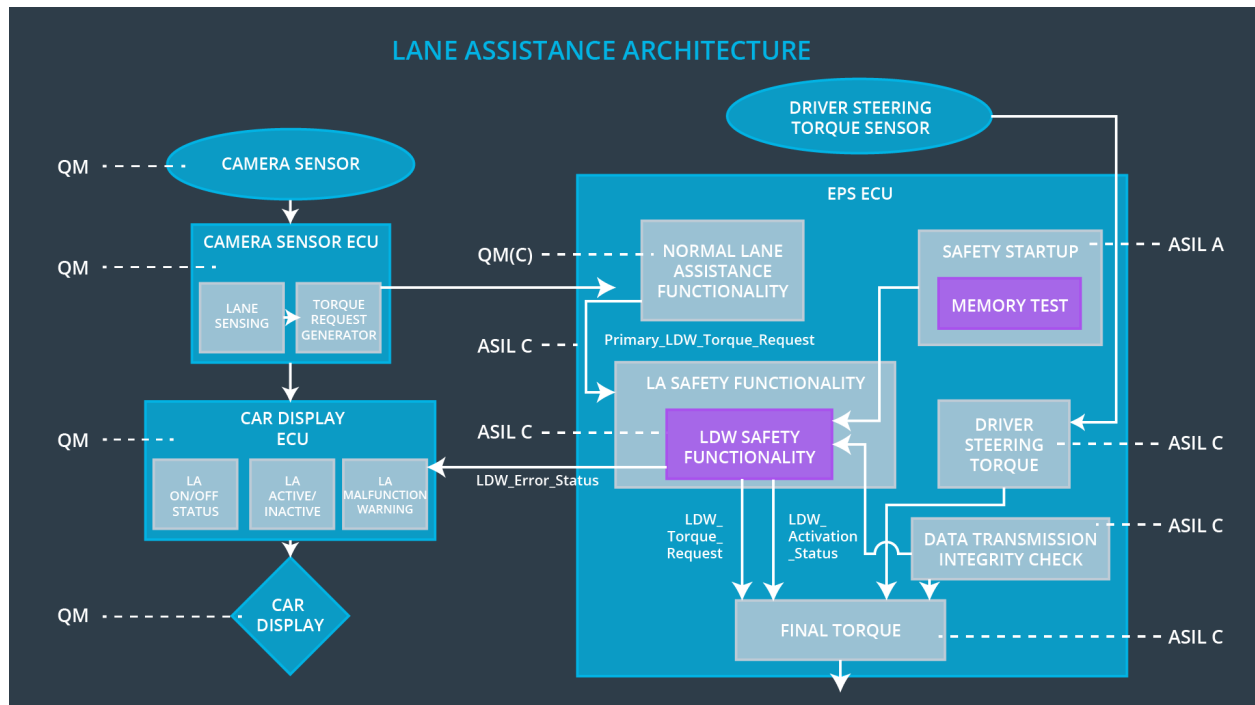| ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LKA safety component shall ensure that 'LKA_Time_Activated_ms' is less than 'Max_LKA_Time_Acitvated_ms'	B	500ms	LKW Safety	'LKA_enable' shall be set to False
Technical	The Validity and integrity of the	B	500ms	Timer	'LKA_enabl

Safety Requirement 02	timer measuring LKA_Time_Activated_ms shall be ensured				e' shall be set to False
Technical Safety Requirement 03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature shall be disabled	B	500ms	LKW Safety	'LKA_enable' shall be set to False
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	LKW Safety	'LKA_enable' shall be set to False
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	Memory Test	'LKA_enable' shall be set to False

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]

All technial safety requirements discussed in this document 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	Turn off	Amplitude exceeds Max_Torque_Amplitude or frequency exceeds Max_Torque_Frequency	Yes	Light on Display
WDC-02	Turn off	Torque applied for longer than Max_Duration	Yes	Note in user's manual