Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
3/14/2018	1.0	David Simon	First attempt
3/21/18	2.0	David Simon	Refined purpose, modified camera sensor ECU description, verify and validate info, delete instructions
3/23/2018	3.0	David Simon	Source content – Udacity lectures, refine purpose, architecture elements, functional safety requirements, recheck allocation
3/24/2018	4.0	David Simon	Guidewords and malfunctions, Safe state, format

Table of Contents

Document history

Table of Contents

Purpose of the Functional Safety Concept

Inputs to the Functional Safety Analysis

- Safety goals from the Hazard Analysis and Risk Assessment
- Preliminary Architecture
  - Description of architecture elements

Functional Safety Concept

- Functional Safety Analysis
- Functional Safety Requirements
- Refinement of the System Architecture
- Allocation of Functional Safety Requirements to Architecture Elements
- Warning and Degradation Concept

Purpose of the Functional Safety Concept

The functional safety concept focuses on minimizing the hazards and potential injury from malfunctions of the electronic lane assistance item consisting of the lane departure warning (LDW) and the lane keeping assistance (LKA) systems. Safety goals, architecture elements, functional safety requirements, validation/verification criteria and methods, warning and degradation concepts are detailed. Descriptions include potential malfunctions, ASIL level, fault tolerant time interval, safe states, and driver warnings.

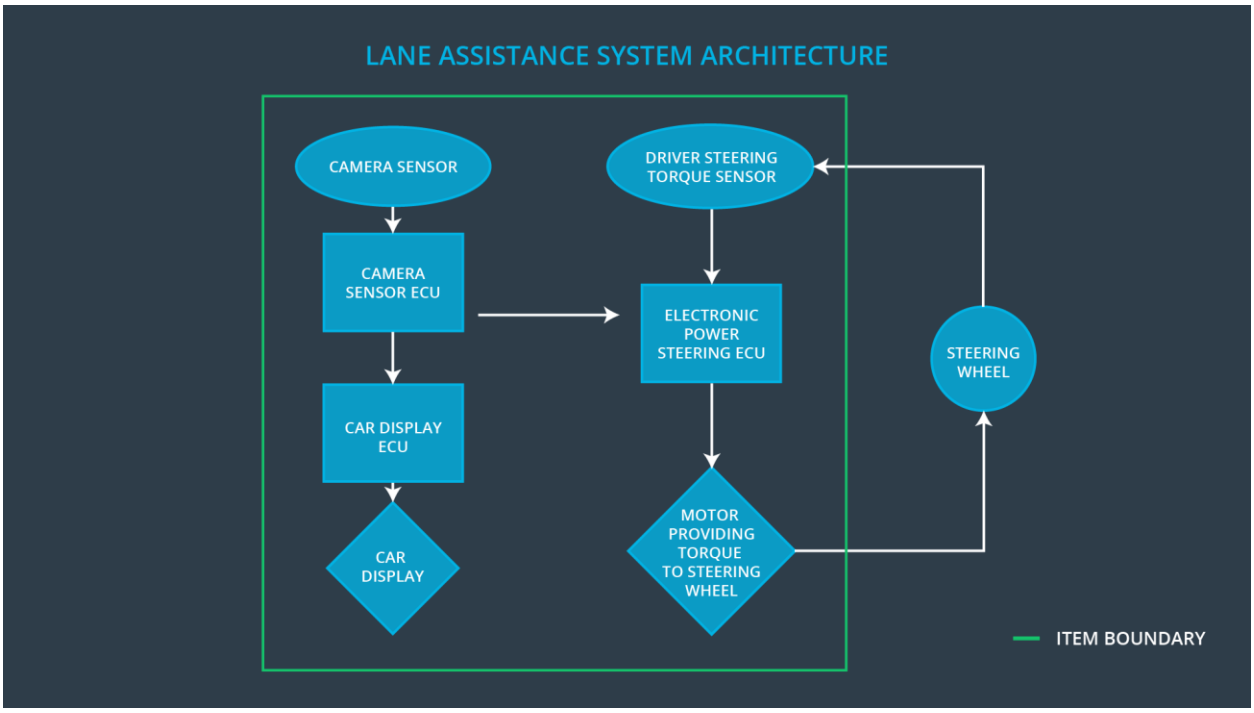
Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

OPTIONAL:
If you expanded the hazard analysis and risk assessment to include other safety goals, include them here.

ID	Safety Goal
Safety_Goal_01	The oscillating steering torque from the lane departure warning function shall be limited.
Safety_Goal_02	The lane keeping assistance function shall be time limited, and the additional steering torque shall end after a given time interval so that the driver cannot misuse the system for autonomous driving.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Detects car location relative to lane lines
Camera Sensor ECU	Processes car location for lane crossing violation as input to electronic power steering ECU and car display ECU
Car Display	Notify driver of operation of lane departure warning and lane keeping assistance systems
Car Display ECU	Processes information from camera sensor ECU for input to car display
Driver Steering Torque Sensor	Senses application of torque to steering wheel for lane departure warning and lane keeping assistance
Electronic Power Steering ECU	Processes information from torque sensor to input to torque motor
Motor	Provides torque to steering wheel for lane departure warning and lane keeping assistance

Functional Safety Concept

The functional safety concept consists of:

- Functional safety analysis
- Functional safety requirements
- Functional safety architecture
- Warning and degradation concept

Functional Safety Analysis

Malfunction ID	**Main Function of the Item Related to Safety Goal Violations**	**Guidewords (NO, WRONG, EARLY, LATE, MORE, LESS)**	**Resulting Malfunction**
Malfunction_01	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback.	MORE	MORE torque than needed. The LDW function applies an oscillating torque with very high torque (above limit).
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback.	MORE	MORE torque than needed. The LDW function applies an oscillating torque with very high torque frequency (above limit).
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane.	NO	NO time limit. The LKA function is not limited in time duration which leads to misuse as an autonomous driving function.

Functional Safety Requirements

Lane Departure Warning (LDW) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 msec	LDW Torque Request Amplitude shall be set to zero.
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 msec	LDW Torque Request Amplitude shall be set to zero.

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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement 01-01	For whatever value we end up choosing for the maximum torque amplitude, we need to **validate** that we chose a reasonable value. We would need to test how drivers react to different torque amplitudes to prove that we chose an appropriate value.	Once we have validated our choice, we then need to **verify** that the safety requirement is met; when the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval. For this specific case, we would probably do a software test inserting a fault into the system and seeing what happens.
Functional Safety Requirement 01-02	For whatever value we end up choosing for the maximum torque frequency, we need to **validate** that we chose a reasonable value. We would need to test how drivers react to different torque frequencies to prove that we chose an appropriate value.	Once we have validated our choice, we then need to **verify** that the safety requirement is met; when the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval. For this specific case, we would probably do a software test inserting a fault into the system and seeing what happens.

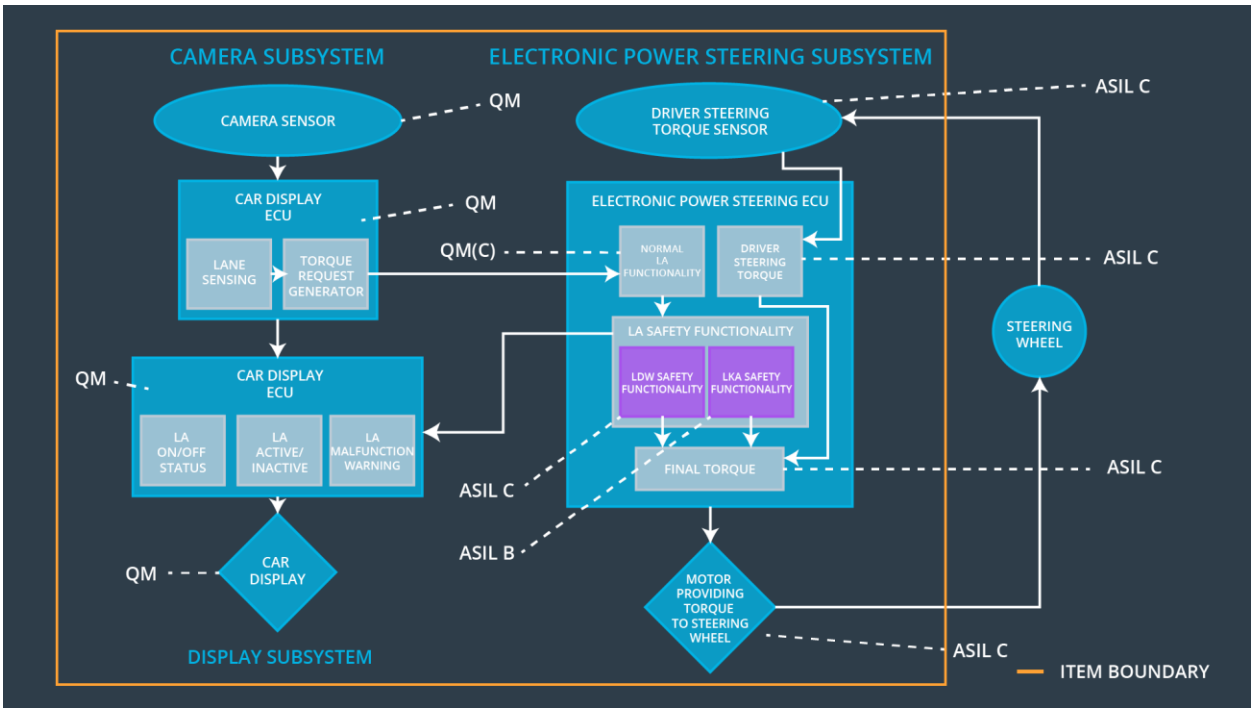
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
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 msec	LKA Torque Request Amplitude shall be set to zero.

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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement 02-01	For whatever value we end up choosing for the maximum duration, we need to **validate** that we chose a reasonable value. We would have to test and validate that the maximum duration chosen really did dissuade drivers from taking their hands off the wheel.	Then we would **verify** that the system really does turn off if the lane keeping assistance exceeded maximum duration. For this specific case, we would probably do a software test inserting a fault into the system and seeing what happens.

Refinement of the System Architecture



Allocation of Functional Safety Requirements to Architecture Elements

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**		
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	**X**		
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	**X**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	LDW off	Malfunction 01 Too high Amplitude Malfunction 02 Too high Frequency	Yes	LDW error light, LDW operation light off
WDC-02	LKA off	Malfunction 03 Max Time Duration Exceeded	Yes	LKA error light, LKA operation light off