Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1

Template Version 1.0, Released on 2017-09-14

D. James

Document history

Date	Version	Editor	Description
2017.09.13	1.0	Denise James	Initial Version of Safety Plan for Lane Assistance
2017.09.28	2.0	Denise James	Added title "Item Lane Assistance Definition" Expanded on the "Development Interface Agreement" section

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of this document is to define an overall safety plan for the Keep Lane Assistance function in compliance with ISO 26262 and to document the roles and responsibilities of the Lane Assistance product team.

Scope of the Project

For the lane assistance project, the following safety lifecycle phases are in scope:

Concept phase
Product Development at the System Level
Product Development at the Software Level

The following phases are out of scope:

Product Development at the Hardware Level
Production and Operation

Deliverables of the Project

The deliverables of the project are:

Safety Plan
Hazard Analysis and Risk Assessment
Functional Safety Concept
Technical Safety Concept
Software Safety Requirements and Architecture

Item Lane Assistance Definition

The Lane Assistance function alerts the driver when the system detects that the vehicle is about to deviate from a traffic lane. This may be done by vibrating the steering wheel, an audio alarm

and lights on the instrument panel. The Lane Assistance system also works in conjunction with the Adaptive Cruise Control system to help the driver steer and keep the vehicle in the lane.

The Lane Assistance Architecture below in Figure 1.

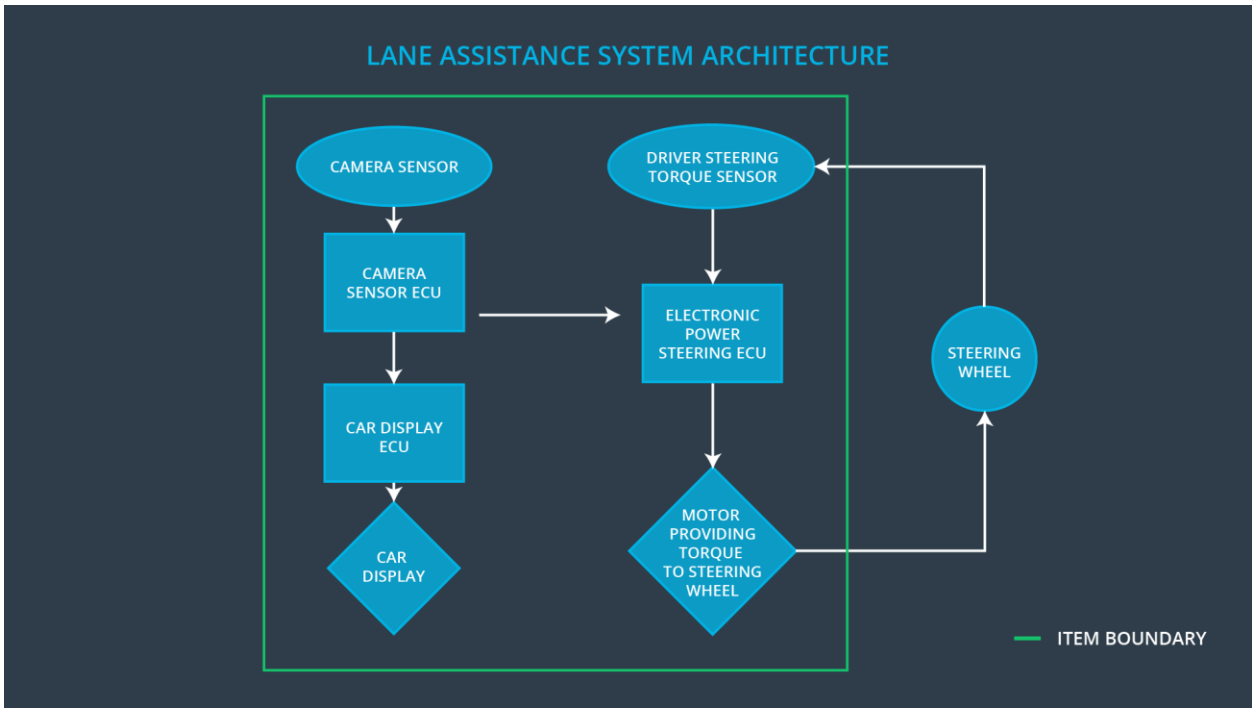

Figure 1 – Lane Assist [1]

The two main functions in Lane Assist are lane departure warning alerts and lane keeping assist.

The Lane Departure Warning Alerts the driver when the vehicle starts to deviate from its lane with a warning buzzer, alert lamp and the application of a small counter-steering force to the steering wheel. The steering wheel vibrates when the driver drifts from the center of the lane by inadvertently.

Lane Keeping Assist is activated when the Adaptive Cruise Control is on and the system senses the vehicle deviating from its lane. Then the system helps the car stay on course near the center of the lane by continuously applying a counter-steering force. This function turns the steering wheel back towards the center of the lane if the driver inadvertently drifts from the center of the lane.

The subsystems for the lane departure warning alerts are the camera subsystem, vehicle display subsystem and the electronic power steering subsystem. The camera sensor information may be sent over a serial vehicle data bus as the ethernet.

The subsystems for the lane keep assist function are the same camera sensor information along with the steering information as angle and torque and adaptive cruise control information.

The boundaries of the Lane Assistance function include the camera, camera ECU, steering wheel, steering ECU, sensor information from the steering wheel, torque applied to the steering wheel, sensor information from the car display panel, display panel ECU and adaptive cruise control information. The elements outside of this system are braking, shifting and accelerating. Of course there are many other electronic elements that are out of this Lane Assistance function as wipers, defrost and air conditioning.

Goals and Measures

Goals

The goal of this document is to define the lane assistance safety plan in accordance with the ISO 26262.

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	Safety Manager Project Manager Safety Auditor Safety Assessor	Constantly
Create and sustain a safety culture	**Safety Manager** Project Manager Safety Auditor Safety Assessor	Constantly
Coordinate and document the planned safety activities	Safety Manager	Constantly

Measures and Activities	Responsibility	Timeline
Allocate resources with adequate functional safety competency	Project Manager	Within 2 weeks of start of project
Tailor the safety lifecycle	Safety Manager	Within 4 weeks of start of project
Plan the safety activities of the safety lifecycle	Safety Manager	Within 4 weeks of start of project
Perform regular functional safety audits	Safety Auditor	Once every 2 months
Perform functional safety pre-assessment prior to audit by external functional safety assessor	Safety Manager	3 months prior to main assessment
Perform functional safety assessment	Safety Assessor	Conclusion of functional safety activities

Safety Culture

The following is from the Udacity Self Driving Car Lecture Notes[2]

"Here are some characteristics of a good safety culture:

- **High priority**: safety has the highest priority among competing constraints like cost and productivity
- **Accountability**: processes ensure accountability such that design decisions are traceable back to the people and teams who made the decisions
- **Rewards**: the organization motivates and supports the achievement of functional safety
- **Penalties**: the organization penalizes shortcuts that jeopardize safety or quality
- **Independence**: teams who design and develop a product should be independent from the teams who audit the work
- **Well defined processes**: company design and management processes should be clearly defined
- **Resources**: projects have necessary resources including people with appropriate skills
- **Diversity**: intellectual diversity is sought after, valued and integrated into processes
- **Communication**: communication channels encourage disclosure of problems"

Safety Lifecycle Tailoring

It is determined what is new in the Lane Assist function and what is carryover from a previous model. We focus only on the changes in functionality and processes in the ISO 26262 standard.

Roles

Role	Org
Functional Safety Manager- Item Level	OEM
Functional Safety Engineer- Item Level	OEM
Project Manager - Item Level	OEM
Functional Safety Manager- Component Level	Tier-1
Functional Safety Engineer- Component Level	Tier-1
Functional Safety Auditor	OEM or external
Functional Safety Assessor	OEM or external

Development Interface Agreement

The purpose of the development interface agreement is to assure all parties are producing safe vehicles in compliance with the ISO 26262 standard.

The responsibilities of our company are to supply a functioning lane assistance system that meets the OEM functional requirements and safety requirements in compliance with the ISO 26262 standard.

From the lecture notes:

"A DIA (development interface agreement) defines the roles and responsibilities between companies involved in developing a product. All involved parties need to agree on the contents of the DIA before the project begins.

The DIA also specifies what evidence and work products each party will provide to prove that work was done according to the agreement.

The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

Here are major sections of a DIA:

- Appointment of customer and supplier safety managers
- Joint tailoring of the safety lifecycle
- Activities and processes to be performed by the customer; activities and processes to be performed by the supplier
- Information and work products to be exchanged
- Parties or persons responsible for each activity in design and production
- Any supporting processes or tools to ensure compatibility between customer and supplier technologies"

Quiz: DIA (Development Interface Agreement)

Confirmation Measures

According to Elektrobit and Udacity Lecture notes

"Confirmation measures serve two purposes:

- *that a functional safety project conforms to ISO 26262, and*
- *that the project really does make the vehicle safer.*

The people who carry out confirmation measures need to be independent from the people who actually developed the project."[3]

A confirmation review "Ensures that the project complies with ISO 26262. As the product is designed and developed, an independent person would review the work to make sure ISO 26262 is being followed."[4]

A functional safety audit assures that the actual implementation meets or exceeds the ISO 26262 requirements.

A functional safety assessment confirms that plans, designs and final project achieves the functional safety requirements.

A safety plan could have other sections that we are not including here. For example, a safety plan would probably contain a complete project schedule.

There might also be a "Supporting Process Management" section that would cover "Part 8: Supporting Processes" of the ISO 26262 functional safety standard. This would include descriptions of how the company handles requirements management, change management, configuration management, documentation management, and software tool usage and confidence.

Similarly, a confirmation measures section would go into more detail about how each confirmation will be carried out.

References

1. Udacity Self Driving Car Lecture Notes

2. Udacity Self Driving Car Lecture Notes

3. Udacity Self Driving Car Lecture Notes

4. Udacity Self Driving Car Lecture Notes