Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 2.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
2018-02-02	1.0	Greg Yeutter	Initial Safety Plan Draft
2018-02-05	2.0	Greg Yeutter	Safety Culture Modification

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of the functional safety plan is to provide a framework for the safety aspects of the Lane Assistance system. In addition, the safety plan assigns functional safety roles and responsibilities for individual job titles.

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 Definition

The Lane Assistance system attempts to determine when a driver has departed a lane unintentionally. The system monitors the vehicle’s position within a lane and also takes driver

intention into account, especially the use of turn signals. The system attempts to alert the driver and to steer the vehicle back into the original “ego” lane.

The Lane Assistance system has two primary roles:

1. Lane Departure Warning: Provides an alert to the driver when a lane is departed unintentionally. In this case, the warning includes a display and a haptic signal provided by applying oscillating torque to the steering wheel.

2. Lane Keeping Assistance: Provides torque to the steering system, attempting to help the vehicle remain in the ego lane.

There are three subsystems involved in the Lane Assistance system. Those are: 1) the camera subsystem, 2) the electronic power steering subsystem, and 3) the car display system. All three subsystems play a role in both the lane departure warning and lane keeping assistance roles.

The system, subsystems, and system boundaries are detailed in Figure 1.

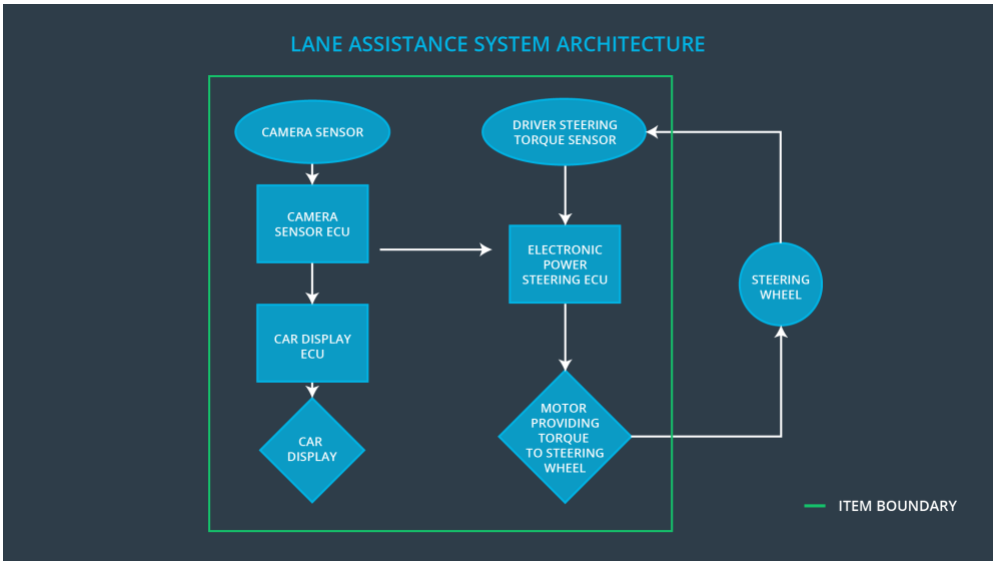

Figure 1: Lane Assistance System Architecture

Goals and Measures

Goals

Vehicles are complex systems with both sociological and technical requirements. Safety includes not only analysis of individual software and hardware components, but also the interaction between systems and subsystems, as well as the safety culture of an organization.

The Functional Safety Plan outlines roles and responsibilities of individual team members, as well as the overarching safety culture of the organization and the product safety lifecycle. ISO 26262 is the standard to which this plan is written.

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	All Team Members	Constantly
Create and sustain a safety culture	Safety Manager	Constantly
Coordinate and document the planned safety activities	Safety Manager	Constantly
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

In this organization, safety has the **highest priority**, greater than other considerations like productivity and cost.

The processes assure **accountability** such that decisions are traceable back to the people and teams who made the decisions. This organization **rewards** the achievement and motivation of functional safety, while **penalizing** shortcuts and decisions that jeopardize quality and safety.

Teams who design and develop products are **independent** from those who audit the work. All stakeholders adhere to **well-defined processes**.

This organization puts an emphasis on **communication** between team members and teams, encouraging early disclosure of potential problems. All projects and teams are allocated the necessary **resources**, including individuals with the appropriate skills, to successfully do their work. **Intellectual diversity** is sought, valued, and integrated into processes.

Safety Lifecycle Tailoring

The following safety lifecycle phases are in scope for this project:

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

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 Development Interface Agreement (DIA) defines the roles and responsibilities between companies developing a product.

The ultimate goal of the DIA is the ensure that all parties contribute to the development of safe vehicles in accordance with ISO 26262. It does this by specifying evidence and work products provided by each vendor to prove work was completed according to the agreement. It also helps avoid disputes, limit liability, and make clear which party should fix safety issues, should they arise.

The Tier 1 vendor will be responsible for:

1. Appointing these positions:
    a. Functional Safety Manager
    b. Functional Safety Engineer
2. Joint tailoring of the safety lifecycle of the Lane Assistance subsystems
3. Analysis of the Lane Assistance subsystems from a functional safety viewpoint
4. Modification of the Lane Assistance subsystems from a functional safety viewpoint
5. Providing tools and/or processes to ensure compatibility with OEM technologies
6. Documentation of all above activities
7. Completion and exchange of the following work products:
    a. Hazard Analysis and Risk Assessment
    b. Functional Safety Concept
    c. Technical Safety Concept
    d. Software Requirements and Architecture
    e. Fully developed and tested subsystems

The OEM will be responsible for:

1. Appointing these positions:
    a. Item Level Functional Safety Manager
    b. Item Level Functional Safety Engineer
    c. Item Level Project Manager
    d. Functional Safety Auditor
    e. Functional Safety Assessor
2. Joint tailoring of the safety lifecycle of the Lane Assistance system
3. Analysis of the Lane Assistance system as a whole from a functional safety viewpoint
4. Modification of the Lane Assistance system as a whole from a functional safety viewpoint
5. Providing tools and/or processes to ensure compatibility with Tier 1 vendor technologies
6. Documentation of all above activities

Confirmation Measures

Confirmation measures ensure that:

- The project and processes conform to ISO 26262
- The project really does improve safety

Those executing confirmation measures must be independent from those who developed the project.

A confirmation review ensures the project complies with ISO 26262. This review is carried out by an independent party.

A functional safety audit ensures the actual implementation of the project conforms to the safety plan.

A functional safety assessment confirms that plans, designs, and developed products actually achieve functional safety.