Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
23AUG17	1.0	Jim Reynolds	Initial safety plan for Udacity Self Driving Car Engineer Nanodegree - Lane Assistance System
23AUG17	1.1	Jim Reynolds	Formatting cleanup, acronyms
23AUG17	2.0	Jim Reynolds	Reviewed document with imaginary team
23AUG17	2.1	Jim Reynolds	Table of contents page numbers

Table of Contents

Introduction

Purpose of the Safety Plan

This plan is intended to ensure that the Lane Assistance System is developed in accordance with functional safety standard ISO 26262.
The system scope and all interested parties will be defined.

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 (LAS) is an Advanced Driver Assistance System (ADAS). There are two primary functions of the (LAS):

1. Lane Departure Warning (LDW)
2. Lane Keeping Assistance (LKA)

LDW

The LDW alerts the driver when the vehicle is on a trajectory to depart the current lane, by vibrating the steering wheel. The LDW is disabled if the driver has activated a vehicle turn signal, as this is indicative of an intentional lane crossing.

The Computer Vision Subsystem (CVS), consisting of a camera, a camera control module, and camera control module software, is responsible for determining the vehicle position with respect to the lane, and requesting the vibrational alert.

The Instrument Cluster Subsystem (ICS), consisting of the instrument cluster (information display), the instrument cluster control module, and the instrument cluster control module software, is responsible for displaying a visual and/or audio alert when the vibrational alert is active.

The Electronic Power Steering Subsystem (EPSS), consisting of a steering wheel input torque sensor, steering wheel motor (torque adder), power steering control module, and power steering control module software, is responsible for measuring the current steering wheel torque applied by the driver, and applying the necessary vibrational torque.

LKA

The LKA assists the driver by turning the steering to maintain the current lane. The LKA is disabled if the driver has activated a vehicle turn signal, as this is indicative of an intentional lane crossing.

The system architecture is the same as LDW.

The LKA is only a temporary driver assistance system, and requires the driver maintain both hands on the steering wheel at all times. The steering assistance shall not be active indefinitely; it is not an autopilot system.

Limitations

Both the LDW and LKA have limitations where visibility is low. The CVS must be able to identify the lane markings with sufficiently high confidence in order for either the LDW or LKA to be enabled. Fog, heavy rain, snow, or poor road maintenance may result in the system not being enabled for periods of time. The CVS is responsible for calculating a lane marking confidence metric and using this as a system enable precondition.

Steering inputs have different effects (lateral acceleration, loss-of-traction, vehicle stability) at varying vehicle speeds. The EPSS is responsible for determining acceptable ranges for

steering angle and rate-of-change of steering angle based on vehicle speed. Above a predetermined speed, LDW and LKA shall be deactivated; the vehicle is being operated outside of validated parameters.

Goals and Measures

Goals

The goal of this project is to ensure that electrical/electronic (E/E) failures of the LDW and LKA systems are safe.

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	All Team Members	Constantly
Create and sustain a safety culture	All Team Members	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

Safety must have the highest priority in the product development. Budgets and timelines may not be altered at the expense of a rigorous safety lifecycle.

Processes must be kept in strict adherence to ensure accountability, consistency, and ultimately, safety.

Teams demonstrating disciplined safety engineering are to be rewarded and recognized.

Teams demonstrating lack of discipline in safety engineering are to be penalized, up to and including termination. Employees who commit to functional safety engineering must understand the gravity of safety, and the mutual trust with the organization.

Safety engineering teams shall be independent (personally, and perhaps geographically) from auditing teams, to ensure a high standard of delivery.

Safety teams are responsible for following all processes as defined by the organization; the organization is responsible for providing tools (hardware, software, storage, equipment) that is required by the processes, and to aid in their execution (e.g. MagicDraw for model-based safety system engineering).

Safety teams shall embrace diversity of ideas, to ensure broad safety coverage. Team members with similar backgrounds or education may tend to have similar ideas for safety that are not complete.

Communication is key. Teams shall regular status meetings, embrace leadership availability and encourage discussion.

Safety Lifecycle Tailoring

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

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 this Development Interface Agreement (DIA) is to ensure that all vehicles are being developed safe, as specified by ISO 26262. There must be no ambiguity about Roles and Responsibilities, to ensure all steps and processes are completed.

The Tier-1 supplier(s) are responsible for developing each of the three main subsystems according to ISO 26262: the CVS, EPSS and the ICS. This includes all hardware and software for each subsystem, as defined above. The Tier-1 supplier(s) are responsible for subsystem-level testing, as well as sub-subystem-level testing (e.g. software unit testing).

The OEM is responsible for the complete LAS. This includes all communication interfaces between subsystems, all ancillary devices (e.g. steering wheel, vehicle speed sensor, CAN bus network, camera mounting hardware, etc.). The OEM is responsible for any signals required to be provided for a given subsystem, such as vehicle speed. The OEM is responsible for testing at the system level (complete LAS testing in-vehicle).

Confirmation Measures

Confirmation measures have two primary purposes: ensure conformance with ISO 26262 and confirm that the safety project indeed increases safety.

The confirmation review satisfies the first purpose above: assuring conformance to ISO 26262. This review is conducted in parallel with the product development.

The functional safety audit confirms that the implementation conforms to the developed safety plan.

The functional safety assement satisfies the second purpose above: assuring that the plans, designs and products achieve functional safety.

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.