Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
03.10.2018	1.0	Nathan Greco	First Draft

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of this safety plan is to define the methodology that will be used in the Lane Assist system to prevent and reduce the occurrence of injuries or negative health impacts that may occur from using this system. This includes but is not limited to the definition of the scope, deliverables, goals, and assignment of responsibilities.

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 system being implemented is a basic **Lane Assist System**. The system includes the hardware and software components necessary to prevent unintentional lane departures that may result in injury to the vehicle operator, passengers, or occupants of any other nearby vehicles. The system includes both a passive and active component, defined by:

- **Lane Departure Warning (LDW)** – The LDW system is the passive implementation of the Lane Assist system. It continuously monitors the lanes on the road and their relative position to the vehicle. If this position exceeds a threshold without use of a turn signal, it interprets this as an unintentional lane departure and vibrates the steering wheel to alert the driver to correct the vehicle path.
- **Lane Keep Assist (LKA)** – The LKA system is the active implementation of the Lane Keep Assist system. The same monitoring conditions are done as above, however, the system will apply a torque to the steering wheel in order to guide the vehicle back onto path itself.

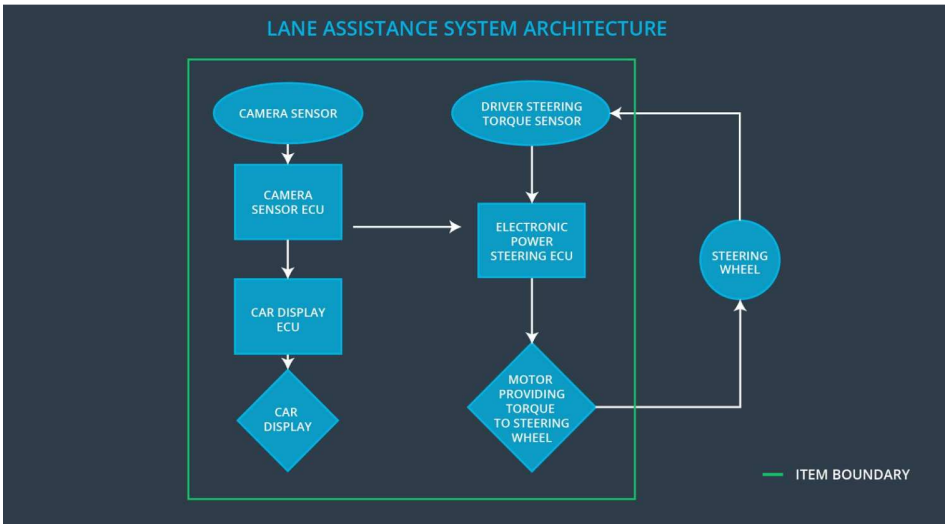

Figure 1: Lane Assist System Architecture

The system can be broken down sub components as shown in figure 1, defined as:

- **Camera sensor** – Camera device that retrieves images of the road in front of the vehicle
- **Camera ECU** – Device which interfaces with camera, steering ECU, and camera display. It is also the processor of the image and interprets the road images with computer vision algorithms to determine the vehicles position relative to the road.
- **Car display ECU** – Controller for the camera display. Receives information from the camera ECU regarding the road line positions and any error or warning messages necessary to indicate.
- **Car display** – This is an informative display to display the road lines and their orientation, display warning and alert messages, and is the primary GUI for the vehicle operator.

- **Driver steering torque sensor** – A sensor that measures that amount of effort the driver is making to steer the vehicle. This is important so that we do not interfere with intentional steering commands from the driver and impede his ability to control the vehicle
- **Power steering ECU** – This is the controller of steering assist motor. It takes input from the camera ECU and steering torque sensor and determines how much of a torque correction, if any, is necessary to correct the current vehicle path.
- **Motor providing torque to steering wheel** – This is the actuator that directly influences the steering of the vehicle. It receives its command from the power steering ECU.
- **Steering wheel** – This is the device which the vehicle operator uses to control the steering angle and path of the vehicle. This device is primarily for manual input from the driver to steer, however the Lane Assist system utilizes it both for lane departure warnings from the LDW system via vibrations and vehicle path corrections via augmented the torque applied by the driver with the torque from the power steering motor.

Goals and Measures

Goals

Generally, it is the goal of this project to minimize the risk of injury to the vehicle operator, passengers, and adjacent vehicle occupants to a level that is acceptable by the general public. Specifically, the implemented system must conform to ISO 26262 – “Road Vehicles – Functional Safety”, a document which defines the life cycle of automotive functional safety and the necessary development process.

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	All Team Members	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

- **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

The safety lifecycle phases will be comprised of the following:

- Concept phase
- Product development for the system
- Product development for the software

The following phases are out of scope of this project:

- Product development for the hardware
- Production and operation of the system

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

An agreement must be made between the OEM and Tier 1 supplier regarding the work content relevant to the functional safety in order to ensure ISO 26262 compliance. See the items below for details on the individual DIA components:

- It is the responsibility of the OEM to appoint a Safety Manager
- It is the responsibility of both parties to jointly develop the safety lifecycle
- It is the OEM's responsibility to:
    - Identify safety manager for the system
    - Identify safety engineer for the system
    - Project management for the system
    - Identify a safety auditor
    - Identify a safety assessor
- It is the Tier-1 supplier's responsibility to:
    - Identify a safety manager for each component
    - Identify a safety engineer for each component
- The deliverables of the OEM to the Tier-1 supplier are:
    - Requirements and functional specifications for each component
    - Cooperation on joint safety lifecycle development
- The deliverables of the Tier-1 supplier to the OEM are:
    - Internal conformance to ISO 26262 for each component
    - Cooperation on joint safety lifecycle development

Confirmation Measures

The intention of the confirmation measures is to:

- Ensure that countermeasures define in both safety assessments and safety audits are implemented
- Ensure that the Lane Assistance project in its entirety and its sub-system level all conform to ISO 26262
- Minimize the risk of injury to the vehicle operator, passengers, and occupants of nearby vehicles to a generally acceptable level when utilizing this system
-

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.