Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.1

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
5 September 2017	1.0	Edward Venator	Initial Submission
16 September 2017	1.1	Edward Venator	Incorporate feedback from initial review

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of this safety plan is to outline the goals, Safety LifeCycle, required resources, process management, and project schedule plan for a Lane Assistance system. This safety plan aims to ensure that the risks of the Lane Assistance system are documented and mitigated, such that the risks are reduced to acceptable levels.

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

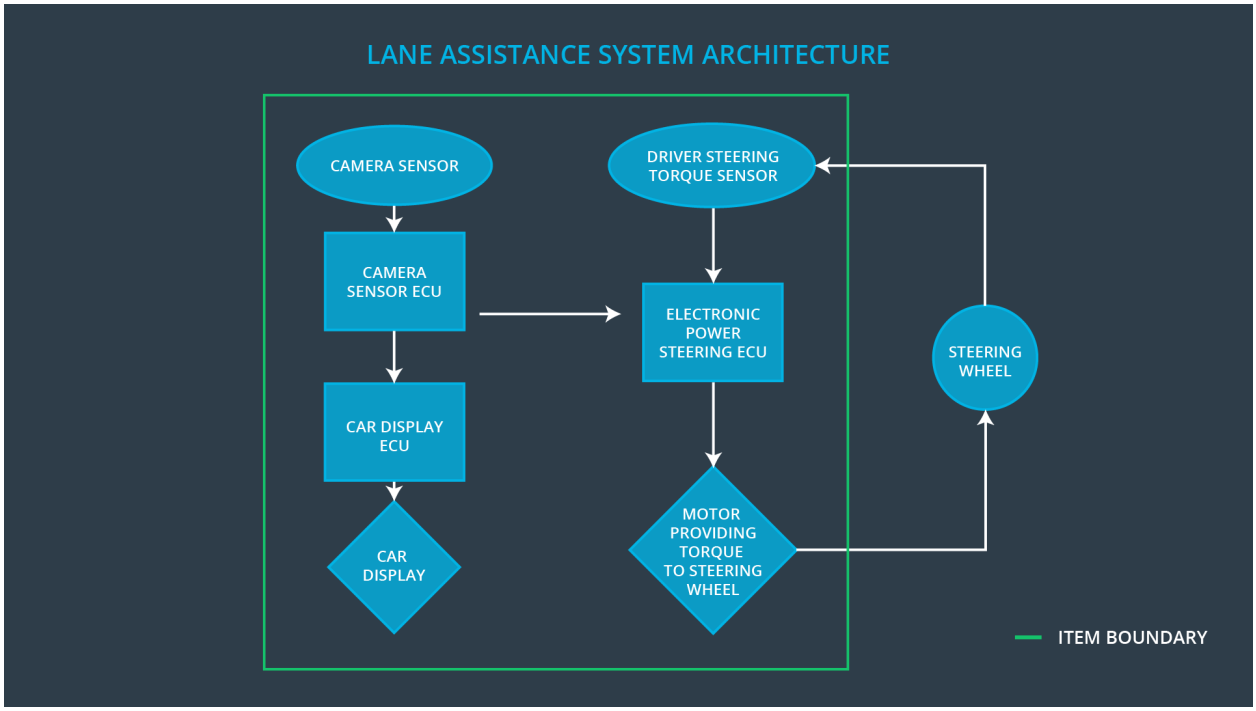
Deliverables of the Project

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 item in question is a Lane Assistance System, which has two functions that assist the driver in maintaining the vehicle's lateral position in the lane. The first function, Lane Departure Warning (LDW), detects when the vehicle drifts towards the edge of the lane and alerts the driver by vibrating the steering wheel. The second function, Lane Keeping Assistance (LKA), detects when the vehicle drifts towards the edge of the lane and moves the steering wheel to turn the vehicle back towards the center of the lane.



The Lane Assistance system is divided into 3 subsystems. The Camera Subsystem detects whether the vehicle is nearing the edge of the lane by processing imagery from a camera. The Camera Subsystem is used for both the LDW and LKA functions. The Electronic Steering Subsystem measures the current position of the steering wheel and applies torque to the steering wheel using an electric motor as required to vibrate the steering wheel for LDW and/or turn the vehicle towards the center of the lane for LKA. The Display Subsystem provides visual feedback to the driver about the functionality and status of both LDW and LKA. Note that the steering wheel itself is outside the boundary of the Lane Assistance item.

Goals and Measures

Goals

The goal of analyzing the lane assistance functions with ISO 26262 is to reduce the risk of the item to an acceptable level. This is accomplished by identifying the hazards that the item may introduce to the system, evaluating the risk of each hazard, and prevent accidents by lowering risks to reasonable levels using systems engineering.

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 is our highest priority, and our safety culture reflects that. Decisions that cut costs or increase productivity must always be analyzed for their safety impact, and safety is never sacrificed for gains in either.

In order to maintain a system of safety accountability, our safety processes are clearly defined, and everyone is properly trained on their responsibilities. All design decisions are traceable to the individual who made the decision. Incentives and rewards are tied to keeping good safety practices and creating safe products. Similarly, failure to follow good safety practices by taking shortcuts that skip safety processes results in penalties. Managers work to make sure that everyone has the proper resources to perform their all of their safety responsibilities, and that the team members performing safety tasks have the appropriate skills.

Communication is key to designing safe products. Team members are encouraged to disclose potential problems whenever they are discovered. In order to maintain the independence of the safety audit process, safety auditors are always separate from the teams who design the product.

Because intellectual diversity is as important to safety analysis as it is to any productive endeavor, this company seeks out team members of various backgrounds and integrates them into the safety review process.

Safety Lifecycle Tailoring

For this project, some phases of the safety lifecycle phase are considered out of scope. Because this project modifies an existing system, it only covers software development for this Lane Assistance System. Therefore, Product Development at the Hardware Level is out of scope. Because this project modifies an existing system, Production and Operation are out of scope. The following safety lifecycle phases remain in scope:

- Concept Phase
- Product Development at the System Level
- Product Development at the Software level

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 (DIA) is to define the roles and responsibilities between the Tier-1 supplier and the OEM.
The OEM is responsible for developing requirements for the vehicle system. The Tier-1 is responsible for developing and producing the system for the OEM.
In this case, the OEM provides a functioning Lane Assistance System. The OEM is responsible for Safety Manager and Safety Engineer duties at the Item level, and the OEM is responsible for project management at the Item level.
The Tier-1 is responsible for analyzing and modifying the subsystems of the Lane Assistance System to ensure that it operates safety with acceptable risk. As such, the Tier-1 supplier accepts responsibility for the duties of the Safety Manager and Safety Engineer at the Component level.

Confirmation Measures

Confirmation measures exist to ensure that this project conforms to ISO 26262 and that the project makes the vehicle safer and not less safe, i.e. the risks have been reduced to acceptable levels. The confirmation measures are composed of a Confirmation Review, a Functional Safety Audit, and a Functional Safety Assessment.
The Confirmation Review ensures that this project conforms to ISO 26262. During the design and development of the system, an independent auditor reviews the work to make sure that the requirements of ISO 26262 are followed.
The Functional Safety Audit ensures that the final implementation of the system conforms to this safety plan. Again, this audit is performed by an independent auditor.

The Functional Safety Assessment ensures that the final implementation of the system achieves functional safety—that is, it makes the system safer and not less safe. This assessment is performed by and independent assessor. It includes both analysis of the plans and design documents and testing the actual system.