Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
22 June 2019	1.0	R. Crane	Initial version.

Table of Contents

Introduction

Purpose of the Safety Plan

This safety plan defines roles and outlines the steps to achieve functional safety in the design of the lane assistance feature.

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 Advanced Driver Assistance System (ADAS) Lane Assistance feature provides (1) a lane departure warning to the driver and (2) provides lane keeping assistance in the form of corrective steering input.

The Lane Assistance system consists of the following subsystems:

1. The **Camera Subsystem**, responsible for providing system with lane detection.
2. The **Power Steering Subsystem**, responsible for providing haptic feedback and control input to the steering wheel.
3. The **Car Display Subsystem**, responsible for providing the user with a visual indication of system activity and an interface for disabling.

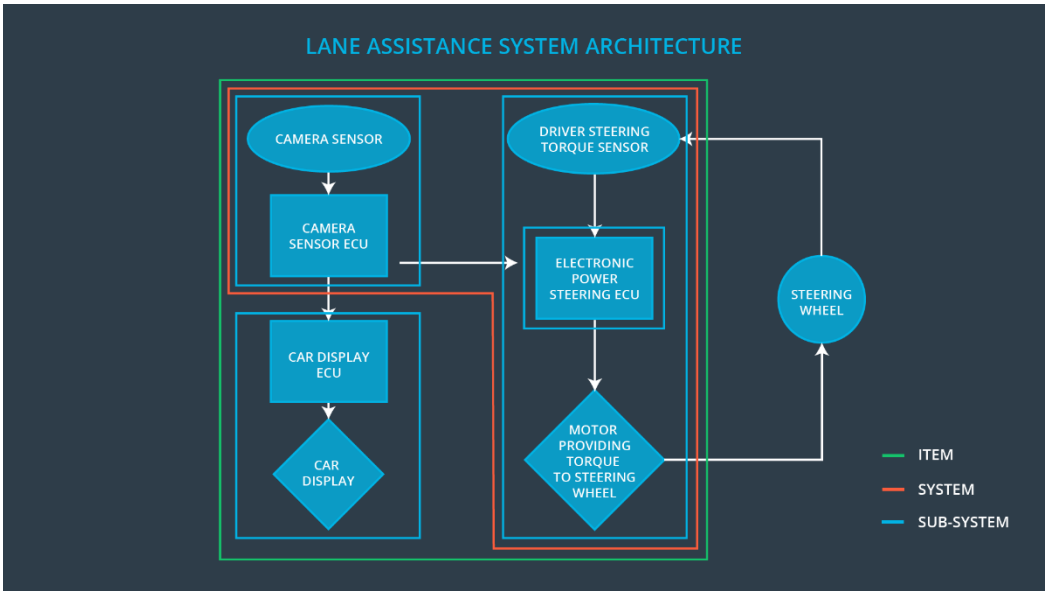

Figure 1. System Architecture

Goals and Measures

Goals

The goal of this analysis is to verify that the design of the electrical and electronic components of the lane assistance function has reduced risk presented by system failures to an acceptable level.

Measures

Achievement of an acceptable level of risk will be proven by rigorous system analysis and testing with inserted failures and degradations.

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 connected to all aspects of operation. Specifically:
Priority: No goal or objective is placed before safety to ensure it is never knowingly compromised.
Accountability: The safety processes are present in every part of the organization and require ownership and approval.
Rewards: Provable safety is an achievement as important as any high visibility demonstration and is consistently reinforced in performance evaluations and compensation reviews.

Penalties: Accountability is reinforced by personal and organizational censures when failures are determined to be reasonably avoidable or negligent.
Independence: The safety organization is vertically independent within the organization.
Well defined: Safety processes are well documented in technical and non-technical presentation
Resources: Safety representatives are present in all organizational units and available for consult.
Diversity: The safety organization includes various engineers and includes rotation from around the company.
Communication: Safety processes and training material is readily available on internal network.

Safety Lifecycle Tailoring

The following phases are in scope for this project:

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

Because no hardware development nor production alteration is expected, it is omitted from this report.

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

This section will define the roles and responsibilities between companies developing the lane assistance system and what evidence and work products will be required.

The OEM must provide analysis of expected system operating conditions. The safety assessment conducted here only analyzes potential failures in components internal to the system. Failures external to the lane assistance feature are not discussed here. Internal failures caused by external faults are assessed only in regard to faults in the system communication interface. Physical or electrical failure caused externally is not analyzed here and is the responsibility of the OEM.

Confirmation Measures

Confirmation measures will ensure that:

- Safety processes comply with the functional safety standard.
- Project execution follows this safety plan.
- Safety is improved by system design.

The confirmation review assesses the above objectives with auditors who are uninvolved with the design or implementation of the system.
A functional safety audit will verify the project implementation conforms to the safety plan.
The functional safety assessment will verify the plans and designs actually achieve functional safety.