Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [4.0]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
12/13/2017	1.0	Pratul Singh	1st attempt
01/06/2018	2.0	Pratul Singh	2nd attempt
01/07/2018	3.0	Pratul Singh	Changes made as per review
01/08/2018	4.0	Pratul Singh	Changes made as per review

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of this safety plan is to provide an overall framework for the Lane Assistance System item and to assign roles and responsibilities for functional safety of this item as defined by ISO 26262 standard.

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

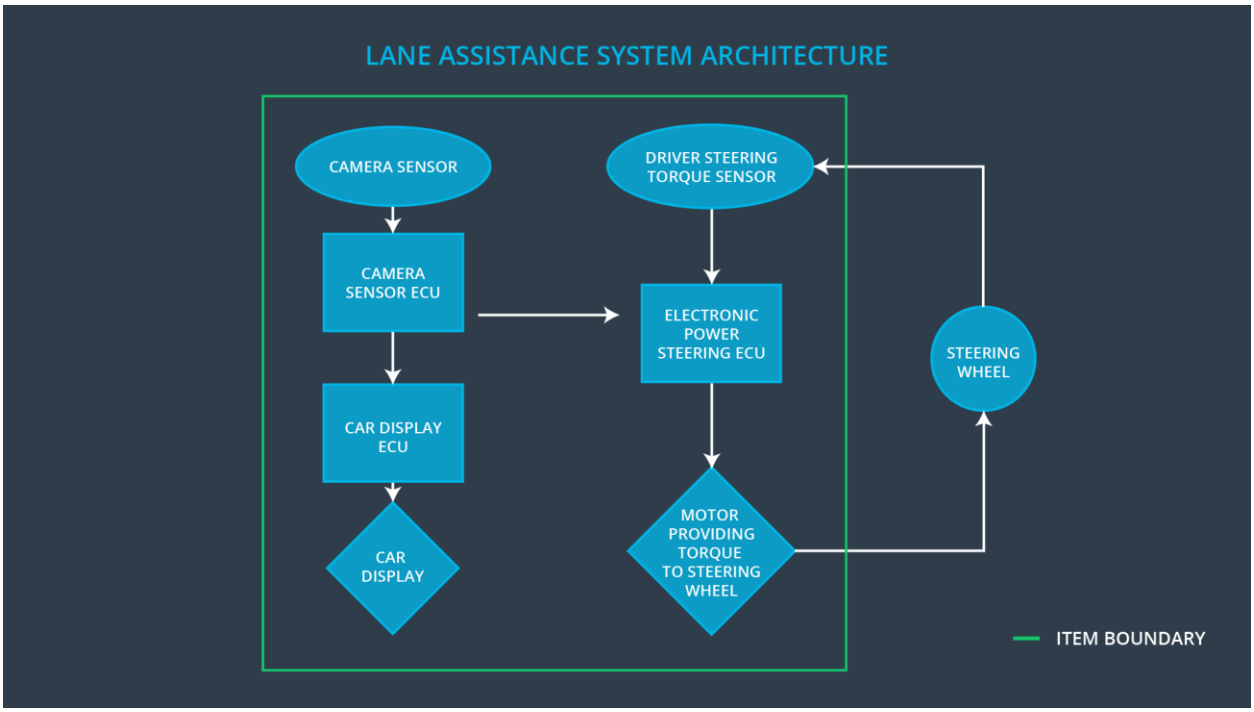
Item Definition

The Lane Assistance Item is a simplified version of an Advanced Driver Assistance System (ADAS) that warns the driver of unintended steering drifts and assists the driver in steering back to the center of the lane. The item will have two functions:

1. Lane departure warning
2. Lane keeping assistance

Lane departure warning: When the driver drift out toward the edge of the lane, the steering wheel vibrates to warn the driver. The vehicle will move the steering wheel back and forward to create vibration.

Lane keeping assistance: When the driver drift out toward the edge of the lane, this functionality will move the steering wheel so that the wheels turn toward the center of the lane. It should apply steering torque to stay in the ego lane (this is the lane where the car is.)
The item boundary includes three sub-systems as shown in Figure 1:
• Camera system
• Electronic Power Steering system
• Car Display system



Goals and Measures

Goals

This project goals are:
- Identify risk and hazardous situations in the Line Assistance system components malfunction causing injuries to a person.
- Evaluate the risks of the hazardous situations.
- Low to risk of the malfunctions to reasonable levels acceptable by current society.

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 Assessor	3 months prior to main assessment
Perform functional safety assessment	Safety Assessor	Conclusion of functional safety activities

Safety Culture

To ensure a safety culture the following characteristics needs to be observed:
- **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

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

This section defines the roles and responsibilities between parties involved in the Lane Assistance project to ensure its development in compliance with ISO 26262.
- **Functional Safety Manager** - Item Level: Pre-audits, plans the development phase for the Lane Assistance item.
- **Functional Safety Engineer** - Item Level: Develop prototypes, integrate subsystems combining them into the Lane Assistance item from a functional safety viewpoint.
- **Project Manager** - Item Level: Allocates the resources needed for the item.
- **Functional Safety Manager** - Component Level (Darien Martinez): Pre-audits, plan the development for the components of the Lane Assistance item.
- **Functional Safety Engineer** - Component Level (Darien Martinez): Develop prototypes and integrate components conforming the Lane Assistance item.
- **Functional Safety Auditor**: Make sure the project conforms to the safety plan.
- **Functional Safety Assessor**: Judges where the project has increased safety.

Confirmation Measures

The purpose of the confirmation measures is:
- Ensure the Lane Assistance project conforms to ISO 26262.
- Ensure the Lane Assistance project does make the vehicle safer.
The Confirmation review ensure the projects comply with ISO 26262. As the product is designed and developed, an independent person would review the work to make sure ISO 26262 is being followed. A Functional safety audit make sure the actual implementation of the project conforms to the safety plan. A Functional safety assessment confirms that the plan, design and developed product 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.