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

23.05.2018	1.0	Arindam Baidya	Initial Attempt

Table of Contents

Introduction

Purpose of the Safety Plan

The Safety Plan helps us to define goals then outline the steps needed to achieve a safe system. This document proposes a safety plan for Lane Assistance item. It appoints the roles and personnel involved in the project. It also defines the scope of the project and sets the timeline in order to successfully complete the Functional Safety of Lane Assistance item in time.

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 consideration is Lane Assistance System which is a part of Advanced Driver Assistance System (ADAS). The Lane Assistance System's responsibility is to warn the driver when the vehicle drifts off the lane (without a turn signal) so as to prevent accidents and maintain safety. It may also automatically take steps to restore the vehicles back to the current lane.

The main functions of the system are:

- **Lane Departure Warning** (LDW)
  The Lane Departure Warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.
- **Lane Keep Assistance** (LKS)
  The Lane Keep Assistance shall apply a steering torque when active in order to stay in ego lane. Ego lane refers to the lane in which the vehicle currently drives.

Both the systems will activate automatically to warn the driver but whenever there is a potentially dangerous situation it shouldn't stop the driver from taking over.

The item also consists of three subsystems:

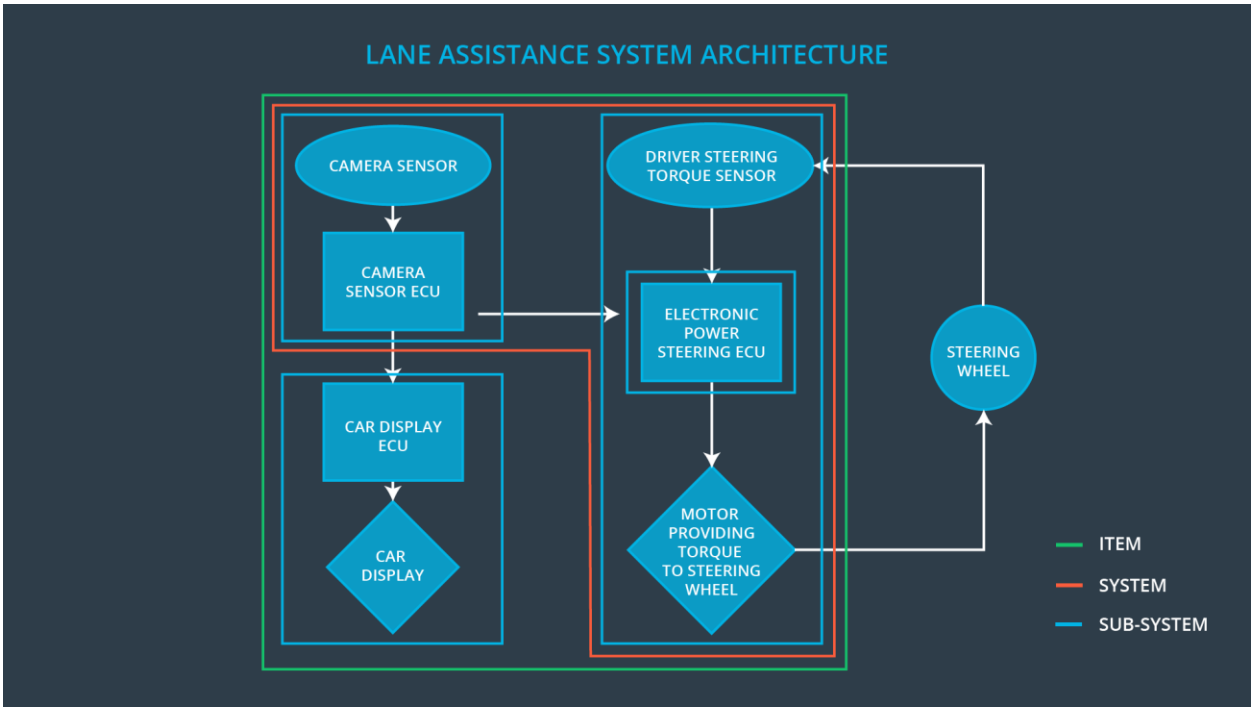
1. Camera system
    a. Camera Sensor
    b. Camera Sensor Electronic Control Unit (ECU)
2. Electronic Power Steering system
    a. Driver Steering Torque Sensor
    b. Electronic Power Steering ECU
    c. Motor providing torque to Steering wheel
3. Car Display system
    a. Car Display
    b. Car Display ECU

The Camera sub-system is responsible for detection and monitoring the position of the vehicle and inform the Car Display and Electronic Power Steering system in case the vehicle moves away from the current lane.

Electronic Power Steering system detects the orientation of the car and adds a steering torque to restore the car back to the center of the lane.

The Car Display system displays the warnings if necessary.

The following diagram shows the different subsystems of Lane Assistance System:



The Line Assistance System does not include the following functionalities:

- Adaptive Cruise Control
- Automatic Parking
- Blind Spot Monitoring
- Tire Pressure Monitoring
- Pedestrian Protection

Goals and Measures

Goals

- 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 a reasonable levels acceptable by current sociality.

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

The following characteristics should be followed to ensure a good 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

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

A DIA (development interface agreement) defines the roles and responsibilities between OEM and tier-1 involved in developing a product. The DIA also specifies what evidence and work products each party will provide to prove that work was done according to the agreement. Both parties need to agree on the contents of the DIA before the project begins. The ultimate goal is to ensure that we are developing safe vehicles 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**: Pre-audits, plan the development for the components of the Lane Assistance item.
- **Functional Safety Engineer - Component Level**: 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 main purpose of confirmation measures are:

- That a functional safety project conforms to ISO 26262, and
- That the project really does make the vehicle safer.

The *Confirmation Review* ensures that the project complies 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.

The *Functional Safety Audit* checks and makes sure that the actual implementation of the project conforms to the safety plan.

The *Functional Safety Assessment* confirms that the plans, designs and developed products actually 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.