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
12/22/2018	1.0	Luis Güette	first document version

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of this safety plan is to provide an overall framework for Lane Assistance System item. Also, it defines roles and responsibilities for players involved in the project.

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:

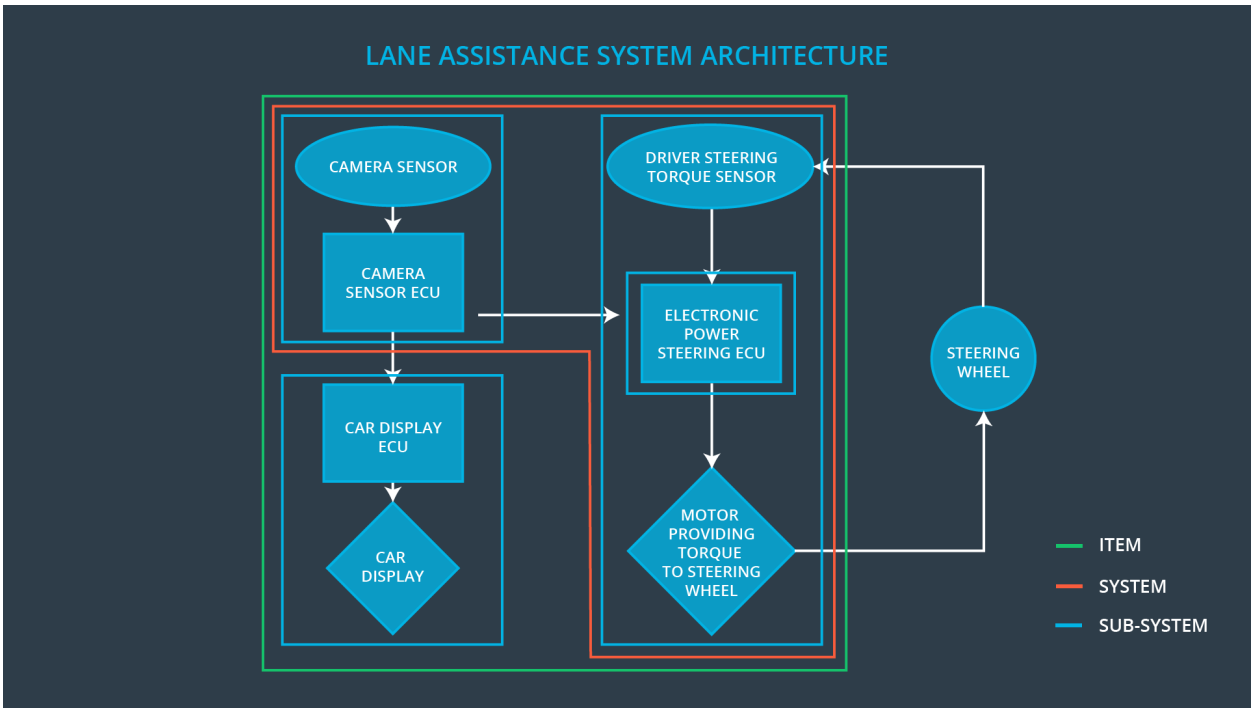
Safety Plan
Hazard Analysis and Risk Assessment
Functional Safety Concept
Technical Safety Concept
Software Safety Requirements and Architecture

Item Definition

When a vehicle leaves the lane, the **Lane Assistance System (LAS)**:

- **Warn** the driver by **vibrating** the steering wheel.
- **Recover** the center of the lane by **moving** the steering wheel.

Below is a diagram about **LAS** architecture:



The diagram shows three sub-systems

- Camera system
- Electronic Power Steering system
- Car Display system

The **Camera System (CS)** is responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake.

The **Electronic Power Steering System (EPSS)** is responsible for measuring the torque provided by the driver and then adding an appropriate amount torque based on a LAS torque request.

The **Car Display System (CAS)** is responsible for showing warnings to the driver and act as a panel control, where the driver can enable or disable vehicle functions.

The camera sense when the vehicle leave the lane, and it sends a signal to the **EPSS** asking to turn and vibrate the steering wheel. The camera sensor will also request to turn on a warning light on the **CAS** dashboard, so the driver knows that the **LAS** is active.

The **EPSS** has a sensor to detect how much the driver is already turning. Then, the **LAS** will apply an extra torque directly to the steering wheel via a motor to get the car back to the center of the lane.

If the driver wants to leave the lane, he must to use the turn signal, and the LAS will be deactivated. The driver can also turn off the **LAS** manually with a button in the display dashboard.

Operational and Environmental Constraints

- Extreme weather conditions (snow, fog, etc), can reduce camera performance.
- Not pre-mapped roads.
- Vehicle electrical energy.
- Complex maneuvers, such obstacle avoidance or automatic lane changing.

Goals and Measures

Goals

The main goals of this project are:

- Identify high risk situations.
- Lower risk to reasonable level.

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

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 companies involved in developing a product. All involved parties need to agree on the contents of the DIA before the project begins.

The DIA also specifies what evidence and work products each party will provide to prove that work was done according to the agreement.

The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

- **Functional Safety Manager- Item Level:**
  - Pre-audits.
  - Planning, coordinating and documenting of the development phase of the safety lifecycle.
  - Maintains the safety plan.
  - Monitors progress against the safety plan.
- **Functional Safety Engineer- Item Level:**
  - Product development.
  - Integration.
  - Testing at the hardware, software and system levels.
- **Project Manager - Item Level:**
  - Acquires and allocates resources needed for the functional safety activities.
  - Overall Project Manager.
- **Functional Safety Manager- Component Level:**

        - Pre-audits.
        - Planning, coordinating and documenting of the development phase of the safety lifecycle.
    - **Functional Safety Engineer- Item Level:**
        - Product development.
        - Integration.
        - Testing at the hardware, software and system levels.
    - **Functional Safety Auditor:**
        - Ensures that the design and production implementation conform to the safety plan and ISO 26262.
    - **Functional Safety Assessor:**
        - Independent judgement as to whether functional safety is being achieved via a functional safety assessment.

Confirmation Measures

Confirmation measures serve two purposes:

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

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.

Functional safety audit: Checks to make sure that the actual implementation of the project conforms to the safety plan is called a functional safety audit.

Functional safety assessment: Confirms that plans, designs and developed products actually achieve functional safety is called a functional safety assessment.

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.