Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
17/05/18	1.0	Trijeet	Initial Draft

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of the safety is to provide an overview of how safe the system is and what measures shall be taken to ensure its safeness. It identifies the responsibilities of personnel that are involved in the functional safety of the lane assistance system, including the steps that are to be performed to adhere to the safety precautions.

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 system is the primary target of this project. The system must have a feedback procedure that warns the driver as and when the car drifts away from the drivable portion of the lane, i.e. towards edges. Ideally the car should drive keeping to the center of the lane. Hence the feedback should assist the driver to keep to the center of the lane or otherwise drive back to the center of the lane whenever the car goes off-center.

The lane assistance system must have at least the following two functions:

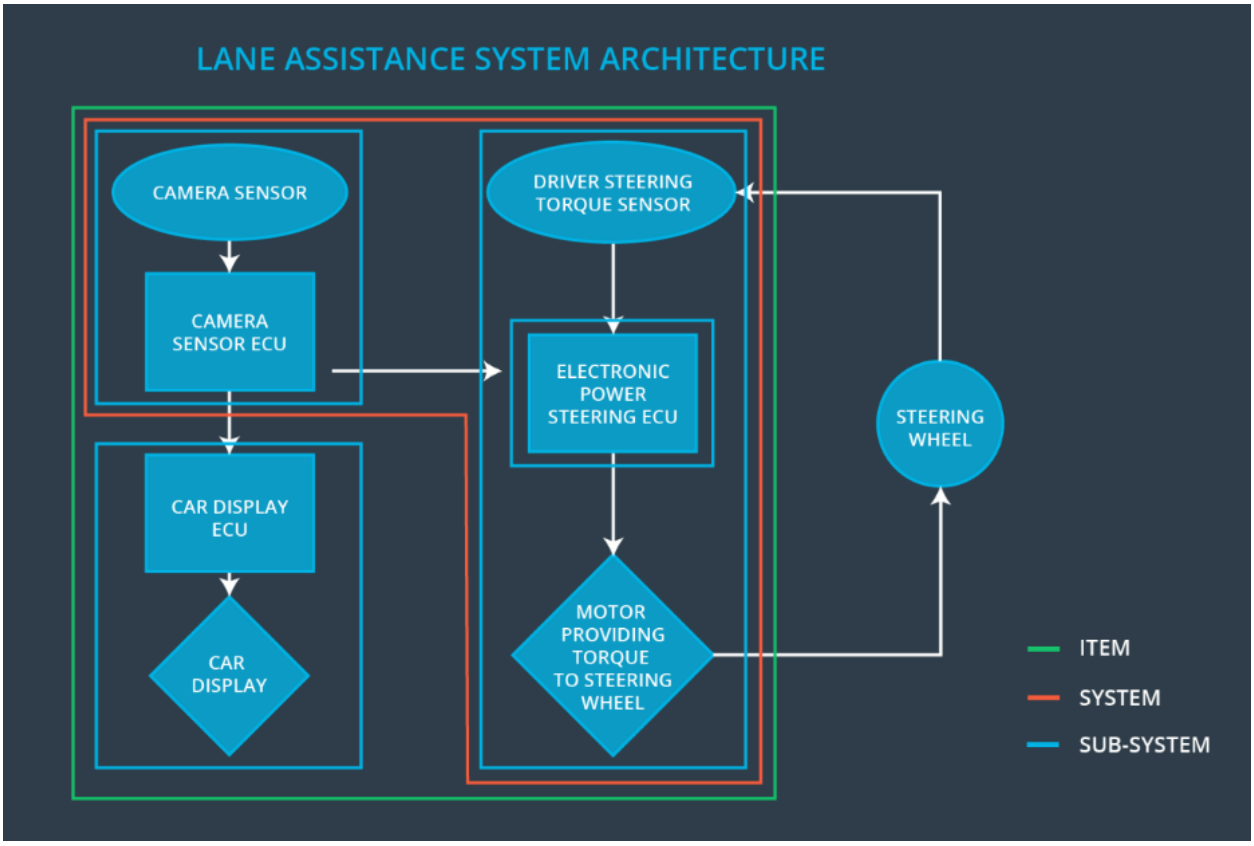
1. **Lane Departure Warning** whenever the car drifts off-center of the lane. This warning may then be translated into a steering torque so as to drive the car back to the lane's center.

2. **Lane Keeping Assistance** to help the car stay on the center of the track as the lane turns. Similar to the above, the assistance function then may be translated to steering torque for the car so that the car turns proportionately to the turn of the lane, thereby preventing over-turning or under-turning.

The above functions are dependent on the following subsystems:

1. **Camera Sensor & ECU**, that senses the lane environment and the car's drift from the lane's center.
2. **Electronic Power Steering ECU**, that takes input from the camera subsystem and calculates the amount of torque required on the steering wheel. The torque is actuated by a motor attached to the steering wheel.
3. **Car Display & ECU**, that provides continuous visual feedback to the driver.

The following diagram describes the boundary and the subsystems inside and outside of it:



Goals and Measures

Goals

The goal in this project is to make sure that the operations of the Lane Departure Warning and Lane Keeping Assistance functionalities operate safely and reliably. This includes identification of potential risks that exists and possible hazards that might occur during operation and finally come up with a plan that minimizes the risks to some reasonably acceptable level.

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

Safety Culture

- **Priority**: We ensure that safety is considered with the highest priority and not just cost and productivity.
- **Accountability**: We ensure that all design decisions are tractable to the respective teams who made the decisions.
- **Rewards**: We encourage employees to notify instances of incorrect process during the development.
- **Penalties**: While meeting functional safety should be mandatory, any negligence in this regard is severely penalized. It may also lead to termination of the employee.
- **Independence**: To prevent any bias, the design & development teams are always kept independent of the audit team.
- **Well defined process**: All design and development processes are well defined and documented.
- **Resources**: We have all necessary resources including employees with appropriate skills who are allocated to this project.
- **Diversity**: Intellectual diversity is always valued in our company.
- **Communication & Disclosure**: Communication between the teams are encouraged with full disclosure of problems.

Safety Lifecycle Tailoring

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

The purpose of the DIA (Development Interface Agreement) is to make sure that each individual or party involved in the development process ultimately delivers a safe product in compliance with ISO 26262.

The responsibility of OEM is to provide with a working lane assistance system and supervise the activities in the scope of project manager, safety manager and safety engineer at the item level. Our company will conduct the activities in the scope of safety manager and safety engineer at the component level.

Confirmation Measures

The purpose of the confirmation measure is to make sure that the processes adhere to the functional safety standards laid down in ISO 26262. It also ensures whether that the project is being executed following the safety plans.

An independent person provides the confirmation review to confirm that the design and development is in complies with ISO26262.

Functional safety audit verifies that the project implementation adheres to the safety plans.

Functional safety assessment analyzes whether the plans, designs and developed products have achieved functional safety or not.

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.