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
24-Aug-2018	1.0	Mohamed Ziedan	Initial Release

Table of Contents

Introduction

Purpose of the Safety Plan

This Safety Plane provides an overall framework for a functional safety "lane assistance system" this includes project schedule plane, confirmation measures, assign roles and responsibilities.

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 question is Lane Assistant,

- It should alert the driver when car departure lane.
- Also, it should move the steering wheel to turn towards the lane center

Main functions

- Lane departure warning.
- Lane keeping assistance

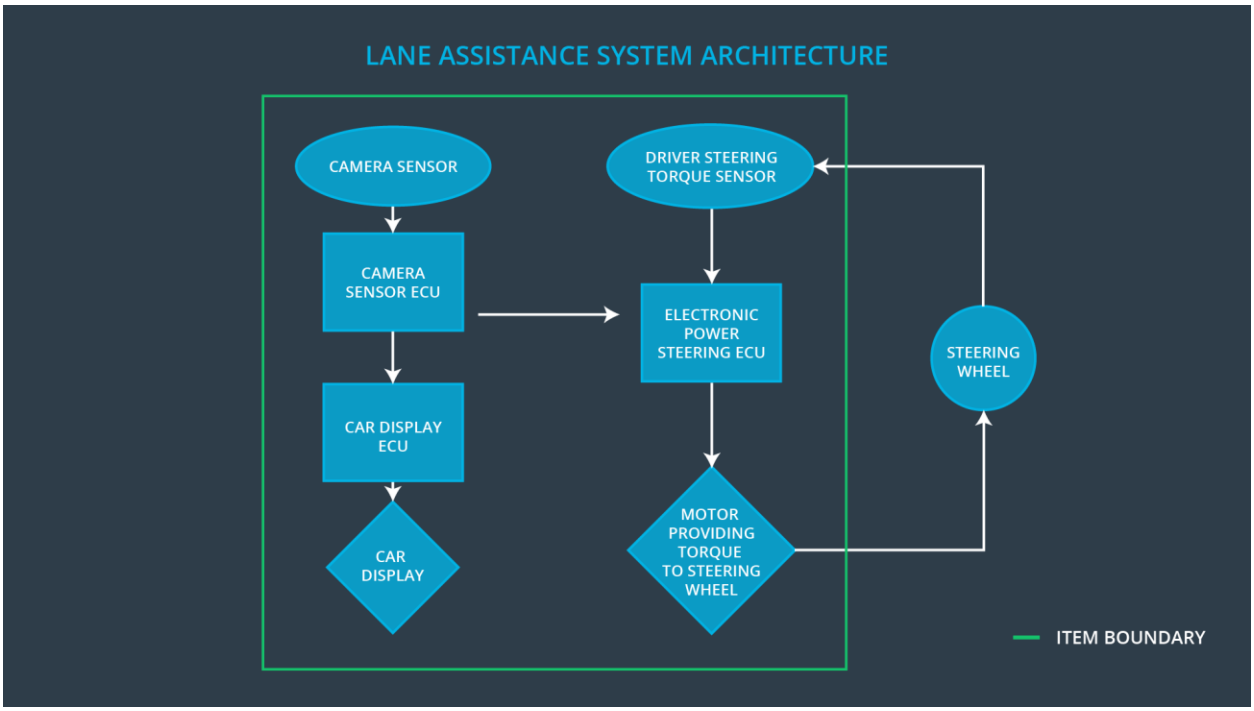
How Do they work

- the lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.
- the lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane**.**

Sub-systems are

- Camera system
  - Responsible of defining lanes.
  - After defining lanes, it will report the car position with respect to the lanes
- Electronic Power Steering system
  - Responsible of keeping the car centered in a lane.
  - Will steer to lane center whenever the car departure the lane enters
- Car Display system
  - Alert Driver with changes in car position.
  - Alert Driver with current steering state/angle.

Boundaries include the 3 subsystems which were mentioned previously (Camera system, Electronic Power Steering system, Car Display system) and the Steering Wheel system.
Only the Steering Wheel system is outside the Lane Assistance item



Some roads may not include lanes
Lanes are difficult to detect in dusty roads
Connected lanes, when road is narrowing (less lanes) or widened (more lanes)

- The driver remains responsible for controlling the vehicle even after LKAS has been activated
- The system is deactivated if the driver applies the brakes.
- The system reactivated after driver release the brakes.

Goals and Measures

Goals

Lane assistance:

- Hazard: car unnecessary leaves lane.
- Goal: car alerts driver and returns to lane center.

Safety Strategy:

- Car uses visual AI to detect lanes, if it leaves lane center for no reason, it MUST provide hepatic feedback to driver, AND proceed correcting this error by going back to lane center.

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	**All Team Members**	Constantly
Create and sustain a safety culture	**Safety Manager, 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

- **High priority**: safety has the highest priority among other constraints like cost and productivity
- **Accountability**: processes ensure accountability such that design decisions are documented and 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 negatively affect 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

Purpose of a development interface agreement

- Clarify the responsibilities of the different parties involved in a functional safety project
- Describe the work products that each company will provide
- Help avoid disputes between companies
- Clarifies who will be responsible for any safety issues in post-production

Our company responsibilities:

- Provides requirements to OEM of what the lane assistance needs to do.
- Test the lane assistance system provided by OEM make sure it will confirm ISO 26262.

OEM company responsibilities:

- Provides lane assistance system matches the requirements and ISO 26262 safety standards.

Confirmation Measures

Confirmation measures serve two purposes:

- Functional safety project conforms to ISO 26262
- The project makes the vehicle safer.

1. **What is a confirmation review?**
   As the product is designed and developed, an independent person would review the work to make sure that the project complies with ISO 26262.
2. **What is a functional safety audit?**
   Checking to make sure that the actual implementation of the project conforms to the safety plan is called a functional safety audit.
3. **What is a functional safety assessment?**
   Confirming 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.