Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0
Template Version 1.0, Released on 2018-06-28

Document history

Date	Version	Editor	Description
2018-6-29	1.0	XU Kuangzheng	Initial Version
2018-6-29	2.0	XU Kuangzheng	Second Version

Table of Contents

Introduction

Purpose of the Safety Plan

- Provide an overall framework for the Lane Assistance item.
- Define roles and responsibilities, ensure each design step not be missed.
- Outline the steps to achieve functional safety.

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

Lane Assistance item alerts the driver that the vehicle has accidentally departed its lane, and attempts to steer the vehicle back towards the center of the lane.

Key points of Lane Assistance System are Lane departure warning and Lane keeping assistance.

When the driver drifts towards the edge of the lane,

- 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.

Lane Assistance item include three sub-systems:

- **Camera system:** Responsible for detecting lane lines and determining when the vehicle leave the lane by mistake.
- **Electronic Power Steering system:** Responsible for measuring the torque provided by the driver and then adding an appropriate amount of torque based on a lane assistance system torque request.
- **Car Display system:** Responsible for display the signal from car display ecu.

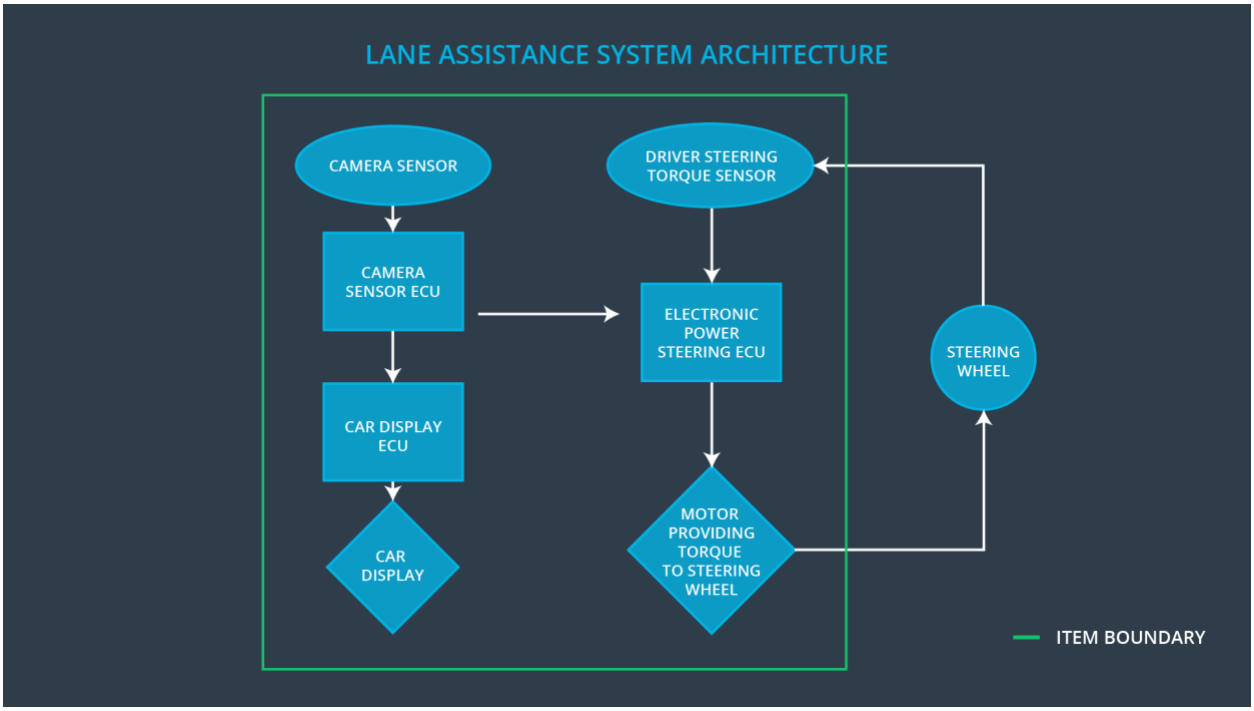

Figure 1 Lane Assistance Architecture

Goals and Measures

Goals

The lane keeping assistance function shall be time limited and the additional steering torque shall end after a given time interval so that the driver cannot misuse the system for autonomous driving.

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	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

Here are some characteristics of 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 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.
The OEM's responsibility to:

- Identify safety manager for the system
- Identify safety engineer for the system
- Identify a safety auditor
- Identify a safety assessor
- Project management for the system
- Supplying a functioning lane assistance system
- Requirements and functional specifications for each component
- Cooperation on joint safety lifecycle development

The Tier-1 supplier's responsibility to:

- Provide functional safety requirements
- Identify a safety manager for each component
- Identify a safety engineer for each component
- Identify a safety auditor for each component
- Identify a safety assessor for each component
- Internal conformance to ISO 26262 for each component
- Cooperation on joint safety lifecycle development

Confirmation Measures

Confirmation measures serve two purposes:

- that a functional safety project conforms to ISO 26262
- 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
Checking to make sure that the actual implementation of the project conforms to the safety plan is called a functional safety audit.

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.
