Safety Plan Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
2017/12/08	1.0	Dongmin Kim	First ver. document about safety plan.

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of the safety plan is to provide an overall framework for the Lane Assistance system, and to achieve functional safety for this system.

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 alerts the driver that the vehicle has accidentally departed its lane, and attempts to steer the vehicle back toward the center of the lane.

The Lane Assistance System will have two functions:
1. **Lane departure warning**: the lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.
2. **Lane keeping assistance**: the lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane.

Include three sub-systems:
- Camera system
- Electronic Power Steering system
- Car Display system
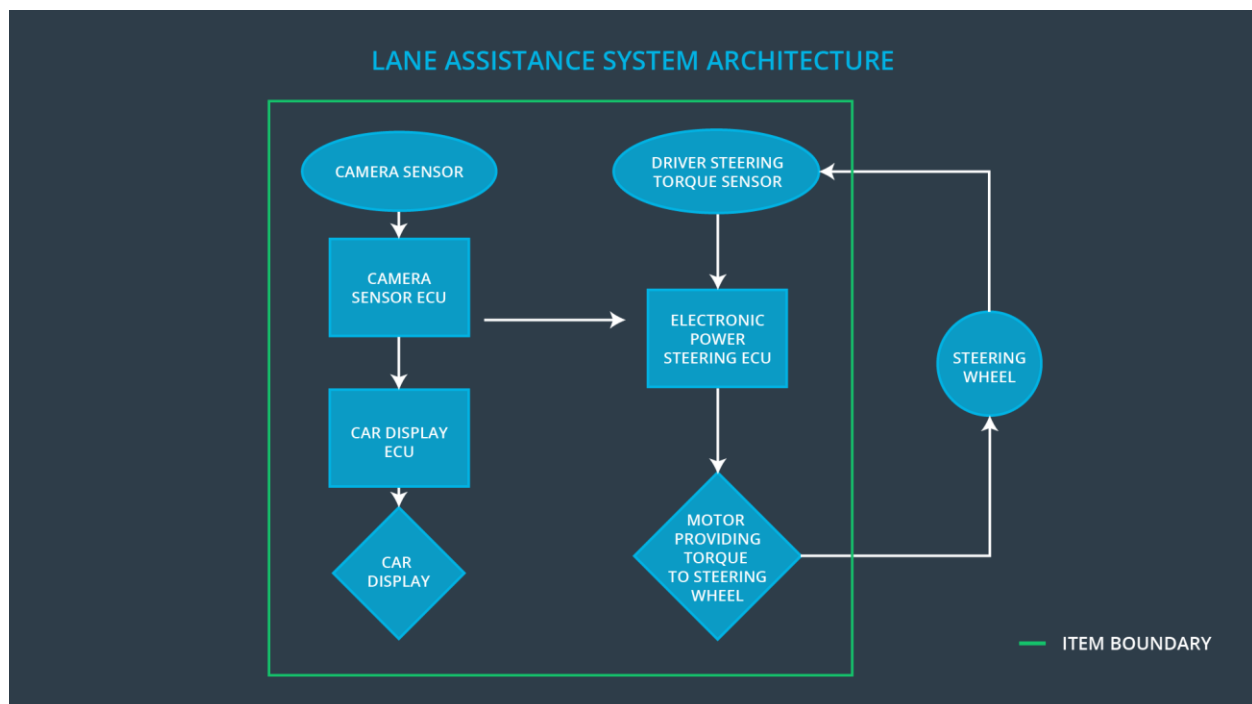
Goals and Measures

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	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

- **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

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 a development interface agreement is to clarify the responsibilities of the different parties involved in a functional safety project, to describe the work products that each company will provide and help avoid disputes between companies.

Responsibilities of Tier-1 is to analyze and modify three sub-systems (Camera system, Electronic Power Steering system, Car Display system) from a functional safety viewpoint.

Responsibilities of OEM is to design and develop the Lane Assistance system in Item level and to audit and assess this project.

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 is to ensure 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 is checking to make sure that the actual implementation of the project conforms to the safety plan.

Functional safety assessment is to confirm that 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.