Safety Plan Lane Assistance

Document Version: [Version]
Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
12-25-2018	0.1	majing	add purposes of safety plan
12-26-2018	0.2	majing	add measurement, safety lifecycle and safety culture
12-28-2018	0.3	majing	add DIA, confirmation measurements
1-2-2018	0.4	majing	add item definition and goals
1-5-2018	1.0	majing	submission

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of safety plan was to outlines the steps to achieve functional safety for vehicle systems, including the following items:

- Scope and deliverables of the project
- Item Definition
- Goals and measures
- Safety culture
- Safety lifecycle tailoring
- Roles
- Development interface agreement
- Confirmation measures.

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

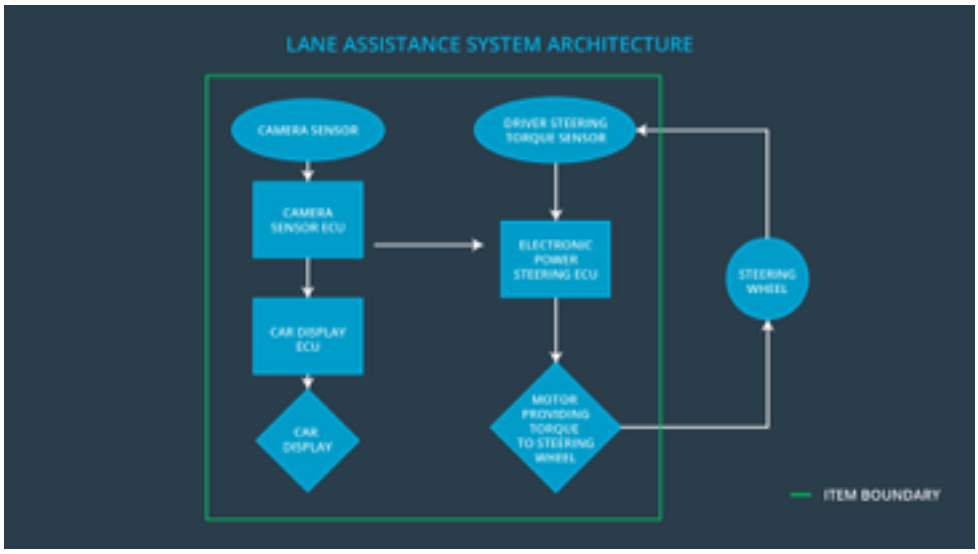
Item Definition

This safety plan is used to cover an ADAS(Advanced Driver Assistance System), which is able to alert the driver to potential danger and control the vehicle to prevent accidents. We call this system the Lane Assistance System. This system has two main functions: lane departure warning and lane keeping assistance.

The lane departure warning function provides the driver a feedback when the car drifts towards the edge of the ego lane by applying an oscillating steering torque. The lane keeping assistance function is able to stay in ego lane when the steering torque is active. These are the subsystems for the item:

- camera subsystem: detect and monitor the position of the car and tell car display and electronic power steering subsystem whether the case drifts towards the edge
- electronic power steering subsystem: detect the driver's operation to make sure the car gets back to the center

This is the diagram of the three subsystems:



Goals and Measures

Goals

- evaluate the risk of dangerous situations
- lower the risk of the malfunctions
- identify dangerous situations in the system malfunction which may cause injuries to a person

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

- High priority: Safety is highest priority
- Well defined processes: Clearly defined management processes and company design
- Accountability: Decisions are documented and traceable
- Diversity: People with different skills and backgrounds work together
- Independence: The auditors and testers belong to a different organization unit than the product designers and developers
- Communication: Potential safety problems have to be reported immediately to the developers for further investigations

The above values are communicated through all management levels to help our employees to archive the functional safety and project goals together.

Safety Lifecycle Tailoring

In scope Lifecycle phases:

- Concept phase
- Product Development at the System Level
- Product Development at the Software Level

Out of scope Lifecycle phases:

- Product Development at 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 Development Interface Agreement (DIA) helps to avoid disputes during planning and development of the lane assistance system as it defines the above roles and responsibilities between the involved companies.

OEM are responsible for overall vehicle safety and all ISO 26262 required functional safety actions. Tier-1 Supplier are responsible for lane assistance component and not the other parts of the vehicle, analyze and modify various sub-systems of the lane assistance component from a functional safety viewpoint. Tier-1 company will act and fix all bugs which apply to the lane assistance system. Functional Safety Managers share the useful information to achieve function safety. All other issues should be investigated by the OEM.

Confirmation Measures

The confirmation measures ensures that the processes comply with the functional safety standard, project execution is following the safety plan and that the design improves functional safety.

The confirmation review ensures that the project complies to ISO 26262 and will be performed by a person which is independent from the design team.

The functional safety audit checks that the actual implementation of the projects conforms to the safety plan.

The functional safety assessment confirms that project plans, designs and development 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.