Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
8/17/2018	1.0	Jun Imamura	First Attempt

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 Item. Especially, following items will be clarified.

1. Target system which is relevant for this project
2. Goal of the project
3. Steps should be taken to ensure the safety
4. Assignment of the roles and responsibility for functional safety
5. Project timeline

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

In this project, the item which we will focus on is “simplified version of Lane Assistance System”

The lane assistance item alerts the driver that the vehicle has accidentally departed the lane and attempts to steer the vehicle back toward the center of the lane.

The item mainly has following two functionalities:

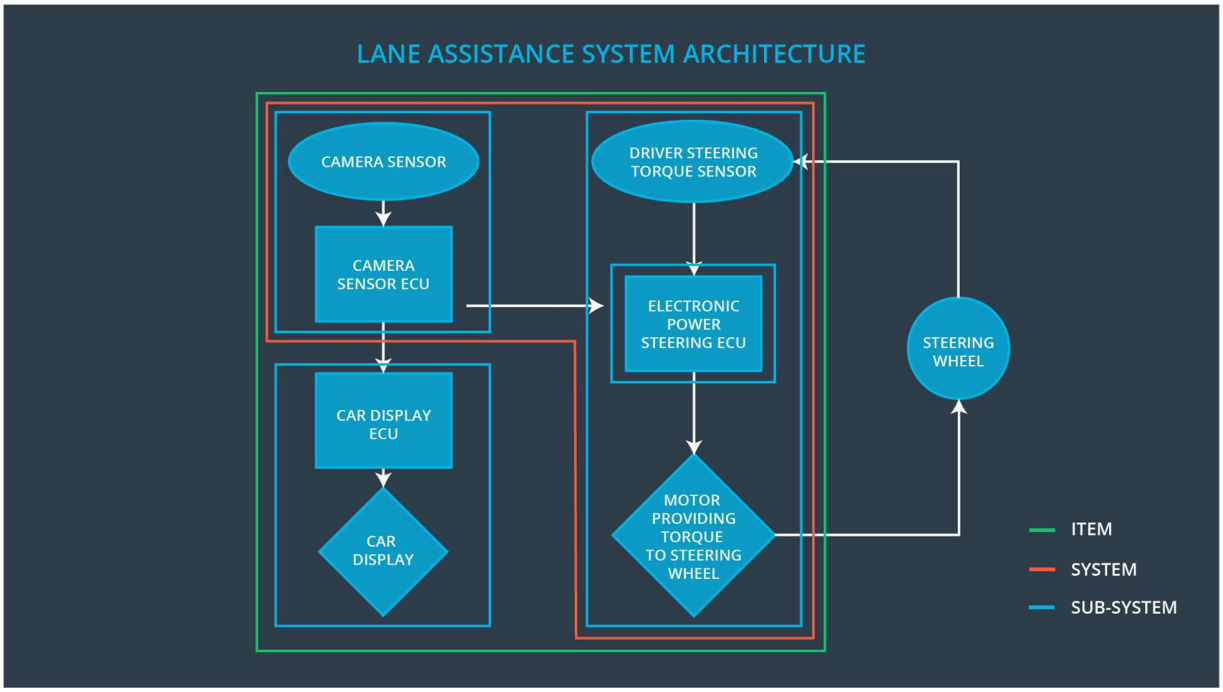
1. **Lane departure warning function**
   When the driver drifts out toward the edge of the lane, the system adds some vibration torque to the steering wheel to provide the driver a haptic feedback.

2. **Lane keeping assistance function**
   When the driver drifts out toward the edge of the lane, the system adds torque to the steering wheel so that the vehicle follows on the center of the lane.

This item is composed of following 3 subsystems:

1. **Camera subsystem**:
   This subsystem is responsible for detecting vehicle position against the edge of the lane, and further divided into two components
   - Camera sensor
   - Camera sensor ECU
2. **Electronic power steering subsystem**
   This subsystem is responsible for applying torque to the steering wheel, and further divided into 3 components
   - Driver steering torque sensor
   - Electronic power steering ECU
   - Motor for providing torque to steering wheel
3. **Car display subsystem**
   This subsystem is responsible for providing information about the status of functionality to the driver, and further divided into 2 components
   - Car display ECU
   - Car display

The following diagram shows the system architecture of this item.



As described above, 3 items are included within this item. This functionality doesn't act as autonomous driving functionality. So the following subsystems/elements will be outside of the item.

- Adaptive cruise control functionality
- Radar to detect leading vehicle
- Lane change assistance
- Side/rear view camera to detect the vehicle on the neighboring lane.

Goals and Measures

Goals

This project goals are:

- Identify risk and hazardous situations when the Lane Assistance system will have malfunction which cause injuries to a person
- Lower identified risks to the acceptable level, which may change according to the situation of society.

Measures

There are several roles to be assigned.

- **Safety manager**
  - Manage safety plan and monitor whether the project follows the plan.
  - Tailor the safety lifecycle and define items related to the project
  - Maintain safety plan
  - Plan pre-audit before audit by safety auditor
- **Product manager**
  - Manage overall project
  - Ensure required resource to implement functional safety
  - Appoint somebody as safety manager
- **Safety auditor**
  - Perform an audit to evaluate if the team followed functional safety standard (This role should be independent from developer)

- **Safety assessor**
  - Do the assessment if the vehicle becomes safer thanks to the functional safety. (This role should be independent from developer)

Above responsibilities can be summarized as follows:

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

In order to realize a safety culture within the team, following characteristic needs to be observed:

- **High priority**: safety should have the highest priority among other constraints like cost and productivity.
- **Accountability**: processes should ensure accountability such that design decisions are traceable back to the people and teams who made the decisions.
- **Rewards**: activity which supports functional safety should be rewarded
- **Penalties**: activity which jeopardize safety or quality should be penalized
- **Independence**: teams who design and develop a product should be independent from the teams who audit the work
- **Well defined processes**: design and management processes within the company should be clearly defined
- **Resources**: necessary resources and skillsets should be secured for the project
- **Diversity**: various viewpoint should be integrated into process
- **Communication**: communication channel should be established so that the problem will be disclosed when it happens

Safety Lifecycle Tailoring

As mentioned in the introduction section, the following safety lifecycle phases are in scope for this project:

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

In order to avoid unnecessary dispute for the product development and implementation, or help identifying who should cope with the particular problem on the product, we need to define Development Interface Agreement (DIA).

OEM and tier-1 supplier respectively have following responsibilities:

OEM:

- Provide functioning lane assistance system
- Ensure functional safety at an item level. Following roles should be appointed from OEM side:
    - Project manager for the system
    - Functional safety manager for the system
    - Functional safety engineer for the system
- Following roles should be appointed from OEM side or external company
    - Functional safety auditor
    - Functional safety assessor

Us as tier-1 supplier:

- Ensure functional safety at a subsystem level. Following roles should be appointed from tier-1 side:
    - Functional safety manager at a component level
    - Functional safety engineer at a component level

Both side:
Other than the above, following items need to be defined and included in the DIA.

- Result of safety lifecycle tailoring which is done jointly.
- Process definition for both sides respectively
- Work product / information to be exchanged / shared
- Process and tools to be used to ensure technical compatibility

Confirmation Measures

Confirmation measures will be done for the following reasons

1. To ensure if the process followed with functional safety standard
2. To ensure if the process followed with defined safety plan
3. To ensure the design contributed to safety

Confirmation measures consist of following activities:

- **Confirmation review**
    - Review by independent person to ensure the design and development followed ISO 26262 standard
- **Functional safety audit**
    - Audit by independent person to make sure the actual implementation of the project conforms to the safety plan
- **Functional safety assessment**
    - Assessment by independent person to ensure that design and development actually achieve functional safety

Note that required independency differs according to the risk level of respective part in the safety lifecycle.

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.